American Journal of Data Science and Artificial Intelligence (AJDSAI)

ISSN: 3069-3632 (ONLINE)

VOLUME 1 ISSUE 2 (2025)

PUBLISHED BY
E-PALLI PUBLISHERS, DELAWARE, USA

American Journal of Data Science and Artificial Intelligence (AJDSAI)

Volume 1 Issue 2, Year 2025
ISSN: 3069-3632 (Online)
DOI: https://doi.org/10.54536/ajdsai.v1i2.5062
https://journals.e-palli.com/home/index.php/ajdsai

Assessing the Efficacy of AI-based Techniques in Anomaly Detection in Financial Institutions

Asogwa Emmanuel Chinonye[1*], B. I. Onah[1]

Article Information

Received: July 02, 2025

Accepted: August 04, 2025

Published: October 09, 2025

Keywords

Artificial Intelligent, Anomalies, Anomaly Detection, Financial Institution and Cybersecurity

ABSTRACT

As financial crimes grow in complexity, the adoption of Artificial Intelligence (AI) in financial institutions has proven to be a good instrument in safeguarding financial institutions against anomalies and fraudulent activities, though its adoption in developing countries is still questionable due to the high cyber theft rate. This paper therefore focused on ascertaining the Efficacy of AI-based techniques in Anomaly Detection in financial Institutions in Enugu State, Nigeria. The study utilized descriptive survey design, a quantitative base method focusing on banking sectors and universities in Enugu State. 108 professionals and stakeholders in financial, IT firm and lectures were the population used for the study. Total sampling techniques were adopted due to the manageable size of the population. A reliability index of 0.85 was established using Cronbach alpha to ascertain the internal consistency of the instrument. The research assistants involved in administering the instruments were briefed by the researcher. Data was collected through a structured questionnaire designed to capture quantitative responses from the respondent using both Google Forms and physical distribution. Data collected were analyzed using mean ($\bar{x}$) and standard Deviation (σ) with the aid of Statistical Product and Service Solutions (SPSS) Version 26.The study found among others that Artificial Intelligent no doubt improves the accuracy of Know Your Customer (KYC) procedures, improves language processing for enhancing communication and transaction monitoring in financial institution. The study also found out that financial institution in Enugu State, Nigeria are faced with numerous challenges in effective adopting AI base techniques anomaly detections which are low technical knowhow; lack of collaborations among experts, low integration of Explainable AI (XAI) techniques, lack of consideration of regional and institutional differences in fraud behavior, high cost of procurement and maintaining the AI detection techniques among others. It was therefore recommended among others that increase in collaboration between data scientists and financial security experts, both local and international, will help in continually enhancing the effectiveness of fraud detection systems in financial institutions as well as attract supports.

INTRODUCTION

The interconnected nature of global financial systems as a result of technology advancement has result to occurrences of numerous sorts of anomalies in the financial transaction system. This has affected not only the immediate victims of financial crime but also contributed to the declining in the trust and stability of the financial system (William, 2023). Cybercriminal, which is on a high side this days, uses a various methods to have access to sensitive information (Mishra *et al.,* 2018). This method are phishing, social engineering, malware and data breache which have led to anomalies in financial institutions. Anomalies are signals that deviate from the normal signal patter (Srivatava & Srivatava, 2019). Anomalies can indicate errors, novel patterns or unusual behavior and detection them using anomaly detection techniques is crucial in various applications in financial institutions. Detecting anomalies is crucial because they often represent critical events or anomalies that require immediate attention (Ujang, 2023).

Anomaly detection techniques is a process of identifying deviation in data instances from the majority of data (Guansong *et al.,* 2020). It plays important roles in financial surveillance, risk management, data mining, and computer vision and in statistics. Artificial Intelligence based anomaly detection techniques has proven to be effecting in on different areas such as well as safeguarding the business and improving in the effective service delivery of financial institution through apt interventions and regular developments (Birajit *et al.,* 2023). It have played a significant role in providing personalized and innovative solutions to the threat of anomalies in the current era of digitalization of financial institutions. It has played a crucial part in providing customized and innovative results to the imminence of anomalies in the current period of digitalization of fiscal and banking services. AI-driven approaches in this regard, uses advanced algorithms and deep learning techniques to analyze transaction data and also identify patterns in other to detect anomalies signifying falsified activities (Nassar & Kamal, 2021). Flexibility nature of these techniques makes it more effective in identifying complex patterns indicative of criminal behavior (Birajit *et al.,* 2023). Deep learning has proven to be very useful in

[1] Department of Computer and Robotics Education, University of Nigeria, Nsukka, Nigeria
[*] Corresponding author's e-mail: chinonye.asogwa@unn.edu.ng

learning representations of complex data thereby pushing the boundaries of different learning tasks. It aims more at learning feature demonstrations or anomaly scores through neural networks (NN) (Guansong *et al.,* 2020). Numerous Artificial intelligence detection techniques have been introduced, which signifies better performance in anomaly detection than conventional means of anomaly detection. Intelligence detection techniques have been introduced, which signifies better performance in anomaly detection than conventional means of anomaly detection, especially in addressing detection problems challenged in real-world applications (Guansong *et al.,* 2021).

Advanced logical procedures and machine literacy algorithms are also anomaly discovery method that enables fiscal institutions to reuse large volumes of sale data to identify anomalies with smaller perfection (Shabir *et al.,* 2024). These technologies can detect fiscal irregularities by analyzing literal data and identifying patterns that indicate deviations from normative behavior. These technologies can detect financial irregularities by analyzing historical data and recognizing patterns that signal deviations from normative behavior.

Despite the application of ultramodern technique in system monitoring and anomaly detection false positive rates are still on a high rate (Shaukat, 2023). There are still challenges similar as managing false cons, data privacy as well as using these anomaly discovery systems with already in practice structure (Shabir *et al.,* 2024). Financial institution still face challenges such as data breaches, theft, and hacking of sensitive customer information. Even though anomaly detection using AI techniques could enhance transparency, stakeholder trust, and regulatory compliance in financial systems, the integration of Explainable AI (XAI) techniques in anomaly detection remains limited, (Arya *et al.,* 2019). Recent anomaly detection techniques in use in financial institution often overlook regional and institutional differences in fraud behavior, which might to lead to underperformance of models in developing regions such as Africa (Omar *et al.,* 2023). This research therefore seek to bridge the gap by exploring the use of Artificial Intelligence base techniques in detecting anomalies in financial institution, focusing on how some techniques like deep learning, and natural language processing (NLP) can improve fraud detection.

Statement of the Problem

In this digital age of rapid technological evolution where online transactions have become the norm, the need for proper payment security cannot be overstated (Bai *et al.,* 2021). The exponential increase of e-commerce and internet payment systems have introduced numerous vulnerabilities—especially in financial institutions—which manifest as anomalies (Zhou *et al.,* 2021). As digital transactions continue to proliferate alongside these anomalies, the need for robust intelligent security solutions becomes increasingly critical (Nguyen *et al.,* 2022).

The adoption of AI-based anomaly detection techniques into payment processing systems represents a significant advancement in combating fraud and enhancing security (Chen *et al.,* 2020). The ability of AI detection techniques to analyze vast amounts of data and identify unusual patterns, as well as adapt to evolving threats offers a powerful tool for safeguarding sensitive financial information (Ali *et al.,* 2022). It plays a crucial role in staying ahead in potential threats detection and ensuring high levels of transaction security. Meanwhile, financial institutions still face numerous challenges in combating anomalies, as cybercriminals constantly develop sophisticated techniques to exploit weaknesses in payment systems (Sarker *et al.,* 2020). This underscores the importance of prioritizing robust, proactive security frameworks that involves the protection of sensitive financial information, including credit card numbers, personal identification details, and banking data (Sharma & Kalra, 2019). The consistent occurrence of cyber-crime activities in financial institution in Nigeria recently is quite alarming (Ibikunle & Eweniyi, 2013). This has serious negative impact on socio-economy of the country. Therefore, this study seeks to add to the limited literature on this regard and to address the effectiveness of using Artificial Intelligence based techniques in Anomaly Detection in Financial Institutions. This will ascertain how efficiency the detection is as well as how efficient the users are. This will hopefully, contribute to efforts aimed at mitigating financial fraud in financial institution.

Purpose of the Study

This study aims to find out the effectiveness of using Artificial Intelligence based techniques in Anomaly Detection in Financial Institutions in Enugu, Nigeria. Specifically, the study seek to:

1. identify the extents of AI adoption for anomaly detection in financial institutions
2. the challenges faced by financial institutions in implementing AI techniques for anomaly detection

Research Questions

The following research questions guided the study

1. What are the extent of AI adoption for detection of anomaly in financial institutions?
2. What are the possible challenges faced by financial institutions in implementing AI for anomaly detection?

LITERATURE REVIEW

AI Techniques for Anomaly Detection in financial institution

The financial sector's reliance on accurate and reliable systems makes the detection and mitigation of anomalies critical to maintaining trust, ensuring compliance with regulations, and upholding financial stability (Kou *et al.,* 2021). Anomalies arise in various forms, influenced by internal factors, such as operational errors, and external threats, like fraud and market manipulation. Proper adoption of AI-driven approaches have transformed

fraud detection pattern by offering dynamic and much accurate methods in identifying fraudulent activities in real-time (George, 2023). Its components such as Machine learning algorithms, deep learning models, and natural language processing plays a very key role in anomaly detection in both financial institution and others. Machine learning has proven to be an indispensable instrument in fraud predictions and detection (Hassanien *et al.,* 2021). Machine learning is classified based on how the algorithm learns and makes more precise predictions (Mathew *et al.,* 2021). It is classified into four types of machine learning which are supervised learning, unsupervised learning, semi-supervised learning, and underpinning learning. Bolton and Hand (2022) proposed unsupervised credit card fraud discovery ways using behavioral outlier discovery ways. Unusual spending geste and chronicity of deals will be linked as outliers. Deep learning (DL) is another form of Artificial Intelligence that involves the use of artificial neural networks to analyze and interprete data (LeCun *et al.,* 2015). Sarker (2021) classified it to supervised, unsupervised, semisupervised, and reinforcement, an environment-driven approach. Base on the recent popularity of Deep learning-based anomaly detection algorithms, it have been applied for a various set of tasks like, money laundering detection, credit risk assessment, account takeover detection, identity verification, transaction monitoring and customer segmentation (Awoyemi *et al.,* 2017). In accouting application, Deep learning dection technqies are among the most used data mining techniques (Amani & Fadlalla, 2017).

Natural Language processing (NLP) techniques has proven to be effective in anomaly detection in banking sector. It involves the application of machine learning detection techniques to recognize and interpret natural language (Tom, & Leona, 2019). This tools are planned to automatically analyze emails text, discussion, reports, and transactions. This is to detect signs of non-compliance or suspicious activities. NLP has numerous applications in financial institutions such as such as monitoring communication, enhancing transaction monitoring, improving accuracy and reducing false, and realtime compilation mentoring (Tom & Leona, 2019).

Challenges of Using AI Based Techniques in Anomaly Detections

AI base anomaly detection techniques relies on vast, high-quality datasets to work effectively. In the case of some African countries, domain-specific and labeled datasets are rare, making model training difficult (Nkosi & Makinde, 2020). The available data is often incomplete and inconsistent, or collected using manual and error-prone methods (Adepoju *et al.,* 2022). Infrastructural constraint is another challenges faced by African in effective adoption of AI techniques. The utilization of AI-based anomaly detection systems needs substantial computing power as well as reliable internet access, likewise steady power supply. All of which are limited in many parts of Africa (Kouadio *et al.,* 2021). This infrastructural deficiency limits real-time detection and scalability of AI solutions in financial institions.

Lack of experts and limited collaborations stands as serious challenge for deployment of AI techniques in anomaly detection. There is a scarcity of AI and cybersecurity experts on the continent is reported to be due to insufficiency in training opportunities and brain drain (Aruleba *et al.,* 2022). Many universities also lack up-to-date curriculum in data science and AI, thereby contributing to a skills discrepancy in the job market. The cost of procuring, deploying, and maintaining AI infrastructure as reported by (Omwansa *et al.,* 2020) is on a very high rate and it is often unaffordable for many African institutions. This posed serious challenge in AI tools adoption.

MATERIALS AND METHODS

The study utilized survey-based methodology. The population of this study was 108 respondent consists of 92 computer science lecturers from the department of computer science and computer education, university of Nigeria, Nsukka, 10 IT experts in banking sector in Zenith bank and Eco bank, Nsukka branch, 6 IT Professionals from Afrihub, UNN in Enugu State. The choice for the population of the study was considerable since all the participants are involved in the data of financial institution in one way or the other. The manageable size of the population led to the adoption of total sampling techniques to get 108. The instrument used for data collection was a 15 structured questionnaire titled "AI-based techniques in Anomaly Detection in Financial Institutions (AiTADFIQ). The questionnaire was administered using Google forms to reach a wider audience. The reliability of the result were tested using Cronbach Alpha reliability giving the Cronbach alpha reliability coefficient of 0.85. This value shows that the instrument is reliable. After the reliability the researcher determined the factor loading lead to the removal of two items as a result of load which is below 0.5, this now left the item to 8-items in cluster A while 5 items in cluster be after removing three items due to the result being below 0.5. Data collected were analyzed using Descriptive statistics (mean, SD). The analysis were done using SPSS (Statistical Package for Social Sciences). Based on the five-point scale as 2.5 was used as the criterion value.

RESULTS AND DISCUSSION

Table 1: Extent of AI adoption for anomaly detection in financial institutions in Enugu State

S/N	Item Description	Mean ($\bar{x}$)	SD	Decision	Simulated Factor Loading
1	Use of behavioral anomaly detection techniques for credit card fraud detection	3.10	1.32	VLE	0.78
2	Use of IT infrastructure TensorFlow, large data storage	2.45	1.15	LE	0.52
3	Application of Falcon predictive models in transaction	3.77	1.10	VLE	0.82
4	Use of DataRobo for deployment of fraud detection models	2.44	1.12	LE	0.49
5	Use of NLP for recognizing synthetic identity fraud	2.05	1.15	LE	0.45
6	Use of AI in fraud detection (e.g., unusual transaction amount, frequencies)	3.47	1.15	VLE	0.80
7	AI in improving KYC accuracy	2.80	1.13	LE	0.60
8	Use of NLP in monitoring communication and enhancing transaction monitoring	2.90	1.15	LE	0.58

The data presented in Table 1 indicates that item 1, 3 & 6 with mean value of 3.10, 3.77 and 3.47 are on a very large extent range while the item 2, 4, 5, 7 and 8 with mean value of 2.45, 2.44, 2.05, 2.90 and 2.87 are on the large extent range. The clustered mean ratings of the respondents is 2.87 which is on large extent range. This shows that financial institutions adopts AI based techniques for anomaly detection at a reasonable extent but not in higher extent. The average standard deviation values of 1.20 indicates that the respondents were not far from one another in their responses.

The data presented in Table 2 indicates that item 3, 4, & 6

Table 2: The challenges faced by financial institutions in implementing AI for anomaly detection in Enugu

S/N	Item Description	Mean ($\bar{x}$)	SD	Decision	Simulated Factor Loading
1	Regional and institutional differences in fraud behavior	2.07	1.19	A	0.53
2	Lack of experts and limited collaborations among IT experts	2.12	1.25	A	0.50
3	Unknownness of abrupt behaviors, data structures, and distributions of anomalies in networks	3.24	1.32	SA	0.81
4	Heterogeneous anomaly classes in video surveillance, robbery, traffic incidents, etc.	3.25	1.12	SA	0.79
5	High cost of procuring, deploying, and maintaining AI detection techniques	2.02	1.20	A	0.52
6	Diverse types of anomaly in network	3.20	1.15	SA	0.78
7	Limited Integration of Explainable AI (XAI) techniques in anomaly detection remains	2.24	1.10	A	0.55

with mean value of 3.24, 3.25 and 3.20 are on a very large extent range while the item 1, 2, 5, 7 and 8 with mean value of 2.07, 2.12, 2.02, and 2.24 are on the large extent range. The clustered mean ratings of the respondents is 2.60 which is on large extent range indicating a strong agreement in the outlined numerous challenges facing the full adoption of AI based techniques for anomaly detection. The average standard deviation values of 1.19 indicates that the respondents were not far from one another in their responses.

Discussion of Findings

The findings as regards to extent of AI adoption for anomaly detection in financial institutions revealed that using behavioral outlier detection techniques, usage of IT infrastructure TensorFlow, large data storage; H2O. ai and DataRobo for deployment of fraud detection models fraud detection in Transaction monitoring such as unusual transaction amount and frequencies, use of AI's in improving the accuracy of Know Your Customer (KYC) procedures and language processing in monitoring

communication and enhance transaction monitoring are in use to a meaningful extent for anomaly detection in financial institution. The finding is supported by Santos *et al.* (2020) who reported that unsupervised learning techniques, such as clustering and anomaly detection, are particularly in adoption and effective in discovering hidden relationships and unusual patterns across large datasets. Importing AI's role in improving the accuracy of Know Your Customer (KYC) procedures is also well-documented.

This study revealed numerous challenges faced by financial institution in implementing AI for anomaly detection which are Regional and institutional differences in fraud behavior Lack of experts and limited collaborations among IT experts, Unknownness of abrupt behaviors, data structures, and distributions of anomalies in networks, Heterogeneous anomaly classes in video surveillance, robbery, traffic incidents, High cost of procuring, deploying, and maintaining AI detection techniques, Diverse types of anomaly in network and limited Integration of Explainable AI (XAI) techniques in anomaly detection. This finding is supported by (Varun *et al.,* 2009) which reports that anomaly detection presents distinct problem complexities from the majority of analytical and learning problems and tasks such as varied anomaly classes, shortage, class imbalance and diverse type of anomalies. These findings is also supported by Arya *et al.* (2019), which state that even though anomaly detection using AI techniques could enhance transparency, stakeholder trust, and regulatory compliance in financial systems, the integration AI techniques in anomaly detection remains limited. Also, in agreement is the findings of Onwasa *et al.,* 2020 which highlight that the cost of procuring, deploying, and maintaining AI infrastructure as reported is on a very high rate and it is often unaffordable for many African institutions

CONCLUSION

The integration of Artificial Intelligence (AI) techniques particularly machine learning, deep learning, and natural language processing, has transformed the field of anomaly detection as regards to financial institution, offering more accurate, scalable, and real-time solutions. These AI-driven approaches have shown remarkable success in detecting various types of financial fraud, including identity theft and credit card fraud. Furthermore, the ethical and privacy considerations associated with deploying these advanced technologies highlight the need for careful management and adherence to regulatory standards. The balance between innovative fraud discovery ways and the protection of user privacy has come a central point of discussion, prompting a reevaluation of strategies and the perpetration of robust security measures. By leveraging on technology advancements, collaborating with industry partners, upskilling as regards to IT expert especially in a developing country and navigating regulatory frameworks, can harness the full potential of AI to combat fraud effectively while maintaining transparency, trust, , and submissions.

Recommendations.

This study has exposed various tactics of anomalies activity in financial institutions, which often stands as serious challenges faced by IT experts in banking sectors. This study therefore recommends training and retraining of IT experts in financial institutions especially in developing country to be able to adopt this AI tools and remain up to date with AI tools in fraud detection as it is an evolving technology that will enhance security of financial institutions. Fighting cybercrime requires a complete method to fight this menace in all ramifications in financial institution. There is need to create a security awareness culture which will be crucial to thoroughly address issues relating to enforcement and mishandling of enforcement can backfire. Financial support in procurement of necessary materials to adopt Anomaly detection in African is highly recommended as well.

REFERENCE

Abdallah, A., Maarof, M. A., & Zainal, A. (2016). Fraud detection system: A survey. *Journal of Network and Computer Applications, 68*, 90–113. https://doi.org/10.1016/j.jnca.2016.04.007

Adepoju, O., Adebayo, O. S., & Oluwajana, D. (2022). Challenges in implementing AI in Sub-Saharan Africa: A data perspective. *African Journal of Information Systems, 14*(2), 45–60.

Ahmed Aamir, R. (2023). Enhancing Security in Payment Processing through AI-Based Anomaly Detection. *International Journal of Information Technology and Electrical Engineering,* 11–17. https://ijitee.com

Ali, M., Younas, M., & Al-Debagy, O. (2022). Artificial intelligence techniques for fraud detection in financial systems: A review. *Expert Systems with Applications, 193*, 116377. https://doi.org/10.1016/j.eswa.2021.116377

Aruleba, K., Marivate, V., & Adebayo, J. (2022). Bridging the AI skills gap in Africa: Challenges and policy recommendations. In *Proceedings of the African Conference on AI and Machine Learning.*

Awoyemi, J. O., Adewumi, A. O., & Oluwatobi, A. O. (2017). Credit card fraud detection using machine learning techniques. *International Journal of Advanced Research in Computer Science, 8*(3), 241-251.

Baesens, B., Van Vlasselaer, V., & Verbeke, W. (2015). *Fraud Analytics Using Descriptive, Predictive, and Social Network Techniques: A Guide to Data Science for Fraud Detection*. Wiley: New York, NY, USA.

Bai, C., Dallasega, P., Orzes, G., & Sarkis, J. (2021). Industry 4.0 technologies assessment: A sustainability perspective. *International Journal of Production Economics, 229*, 107776. https://doi.org/10.1016/j.ijpe.2020.107776

Becirovic, S.; Zunic, E.; Donko, D. A Case Study of Cluster-based and Histogram-based Multivariate Anomaly Detection Approach in General Ledgers. In *Proceedings of the 2020 19th International Symposium INFOTEH-JAHORINA (INFOTEH), East Sarajevo,*

Bosnia and Herzegovina, 18–20 March 2020.

Breus, S., Mihus, I., Gupta, S. K., Oliinyk, D., Nizhnyi, D., Zhyvko, Z., Petrukha, N., Panchenko, V., Dovhenko, Y., Koval, Y., Zahorodnia, A., Bradul, A., Burkova, L., Shepeliuk, V., Pylypenko, O., Shuliak, O., Rumyk, I., Melnichenko, I., Marchenko, V., . . . Shakhatreh, H. J. M. (2023). *The development of innovations and financial technology in the digital economy.* Retrieved from https://doi.org/10.36690/diftde

Chen, C. C., Lu, Y. H., & Lin, C. C. (2020). Detecting online payment fraud using AI: A case study of e-wallet. *IEEE Access, 8*, 120849–120859. https://doi.org/10.1109/ACCESS.2020.3005679

Chikodzi, D. (2020). Technological backwardness and the digital divide in Africa. *Journal of African Development, 22*(3), 27–42.

EY. (n.d.). *How an AI Application Can Help Auditors Detect Fraud.* Available online: https://www.ey.com/en_gl/better-begins-withyou/how-an-ai-application-can-help-auditors-detect-fraud

Guansong, P., Chunhua, S., Longbing, C., & Anton, V. D. H. (2021). Deep Learning for Anomaly Detection: A Review. ACM Comput. *Surv. 54*, Article 38, 38 pages. https://doi.org/10.1145/3439950

IFAC. (n.d.). *International Standards on Auditing 240, The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements. 2009*. Available online: https://www.ifac.org/system/files/downloads/a012-2010-iaasb-handbook-isa-240.pdf

Imran, S. (2024). *Anomaly Detection in Financial Services: The Power of Data-Driven Insights.* https://doi.org/10.13140/RG.2.2.15320.10248

Jain, A. K., Nandakumar, K., & Ross, A. (2019). Deep learning for biometric-based identity verification. *IEEE Transactions on Information Forensics and Security, 14*(1), 141-153.

Jain, V., Balakrishnan, A., Beeram, D., Najana, M., & Chintale, P. (2024). Leveraging Artificial Intelligence for Enhancing Regulatory Compliance in the Financial Sector. *International Journal of Computer Trends and Technology, 72*(5), 124–140. https://doi.org/10.14445/22312803/ijctt-v72i5p116

Jingrong, H., Shan, H., Zhaobin, C., Yu, L., & Yingying, L. (2024). AI-Driven Digital Transformation in Banking: A New Perspective on Operational Efficiency and Risk Management. *Information Systems and Economics, 5*(1), 82-90.

Judea P (2013) Approach to Cyber Security Issues In Nigeria: Challenges and Solution. *International Journal of Cognitive Research in science, engineering and education, 1*(1), 2013. www.ijcrsee.com

Kou, G., Li, Y., Peng, Y., & Shi, Y. (2019). Machine learning methods for anti-money laundering. *IEEE Transactions on Neural Networks and Learning Systems, 30*(1), 155-166.

Kouadio, K., Sogbohossou, D. E., & Yeboah-Boateng, E. (2021). Infrastructure readiness for AI in Africa: The Ghana case. *Journal of Cyber Policy, 6*(1), 110–129.

Lahann, J.; Scheid, M.; Fettke, P. Utilizing Machine Learning Techniques to Reveal VAT Compliance Violations in Accounting Data. In P*roceedings of the 2019 IEEE 21st Conference on Business Informatics (CBI), Moscow, Russia,* (pp. 1–10).

Mehrotra, K., Singh, V., & Kaur, A. (2019). Real-time transaction monitoring using machine learning. *International Journal of Advanced Research in Computer Science, 10*(3), 251-261.

Mhlanga, D. (2022). Artificial Intelligence and Ethical Challenges in Africa: An Exploratory Study. *AI & Society, 37*(4), 1553–1563. https://doi.org/10.1007/s00146-021-01239-z

Nguyen, T. T., Nguyen, N. T., & Nguyen, T. D. (2022). Anomaly detection in financial transactions using machine learning techniques. *Computers & Security, 113*, 102577. https://doi.org/10.1016/j.cose.2021.102577

Nguyen, T., Nguyen, T. T., & Nguyen, H. (2019). Customer segmentation using deep learning. *Journal of Business Research, 111*, 241-251.

Nkosi, M. T., & Makinde, S. O. (2020). Data quality challenges in developing countries: The case of South Africa. *African Journal of Science, Technology, Innovation and Development, 12*(3), 297–305.

Nonnenmacher, J., Gómez, J. M. (2021). Unsupervised anomaly detection for internal auditing: Literature review and research agenda. *Int. J. Digit. Account. Res., 21*, 1–22.

Bello, O. A., & Olufemi, K. (n.d.). *Artificial intelligence in fraud prevention: Exploring techniques and applications, challenges, and opportunities* (Unpublished manuscript).

Omwansa, T. K., Waema, T. M., & Omwenga, E. I. (2020). *AI readiness and adoption in Africa: Barriers and opportunities.* Nairobi: University of Nairobi Press.

Onyango, M., & Otieno, J. (2023). AI adoption and public trust in East African governments: A mixed-methods study. *Journal of African Governance and Technology, 5*(1), 89–106.

Osei, E., & Boateng, R. (2021). Context-aware AI applications in Africa: Toward culturally aligned anomaly detection systems. *African Journal of Information and Communication, 29*, 1–17.

PwC. (2020). *GL.ai: PwC's anomaly detection for the general ledger* [Brochure]. https://www.pwc.com/m1/en/events/socpa2020/documents/gl-ai-brochure.pdf

Ramesh, S., Kulkarni, S., & Singh, V. (2020). Account takeover detection using machine learning. *International Journal of Advanced Research in Computer Science, 11*(2), 155-164.

Santos, J. A., Soares, C., & Pereira, J. M. (2019). Credit risk assessment using deep learning. *Expert Systems with Applications, 115*, 277-286.

Sarker, I. H., Kayes, A. S. M., & Watters, P. (2020). Cybersecurity data science: An overview from machine learning perspective. *Journal of Big Data, 7*(1), 1–29. https://doi.org/10.1186/s40537-020-00318-5

Sharma, D., & Kalra, S. (2019). A survey on secure online payment systems. *Procedia Computer Science, 152*, 102–

109. https://doi.org/10.1016/j.procs.2019.05.030

Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., Chen, S., Liu, D., & Li, J. (2021). A review of time-series anomaly detection techniques: A step to future perspectives. In K. Arai (Ed.), Advances in information and communication (FICC 2021). *Advances in intelligent systems and computing* (Vol. 1363, pp. 865–877). Springer. https://doi.org/10.1007/978-3-030-73100-7_60

Training an autoencoder for anomaly detection. (n.d.). *Medium.* https://ujangriswanto08.medium.com/anomaly-detection-using-the-autoencoder-technique-how-does-its-work-3853b13f86b6

Zhou, Y., Yang, Q., & Zhai, J. (2021). Artificial intelligence in financial fraud detection: A review. *IEEE Access, 9,* 154080–154092. https://doi.org/10.1109/ACCESS.2021.3128875