ADOPTION OF ARTIFICIAL INTELLIGENCE IN CURBING FRAUD IN PUBLIC ORGANISATION: ASSESSING FRAUD DETECTION AND CONTROL

KING C. HUGE, Ph.D
DEPARTMENT OF VOCATIONAL STUDIES
FACULTY OF EDUCATION
UNIVERSITY OF ROCHESTER
ROCHESTER
NEW YORK CITY
And

OBOT, EDIONGSENYENE GODWIN
DEPARTMENT OF ACCOUNTANCY
SCHOOL OF BUSINESS AND MANAGEMENT

Abstract

This study examined the adoption of artificial intelligence in curbing fraud in public organisations, assessing fraud detection and control. Several essential concepts were reviewed in the course of this study, which included artificial intelligence, fraud, fraud detection, fraud control, and types of fraud in public organisations, among others. The study highlighted that the integration of artificial intelligence (AI) in fraud detection and control represents a significant advancement in the fight against financial malfeasance within public organizations. The study mentioned that AI fraud detection operates by implementing machine learning algorithms that are designed to analyse behaviours and detect anomalies indicative of fraud, and that AI has transformed fraud detection and control, helping public organisations combat fraudulent activities by offering sophisticated methods to detect, prevent, and mitigate risks. Furthermore, the study outlined the effects of artificial intelligence on fraud detection and control, which include improved detection accuracy, real-time monitoring, reduced false positives, and adaptive security measures. The study concluded that the integration of artificial intelligence (AI) in fraud detection and control is a significant advancement in combating financial malfeasance in public organizations. One of the recommendations of the study was that public organisations should allocate resources to acquire and maintain cutting-edge AI technologies and infrastructure.

Keywords: Artificial Intelligence, Fraud, Public Organization, Detection and Control

Introduction

The integration of artificial intelligence (AI) in fraud detection and control represents a significant advancement in the fight against financial malfeasance within public organizations. In recent years, the complexity and sophistication of fraudulent schemes have escalated, making traditional detection methods increasingly inadequate. AI, with its advanced data analytics and pattern recognition capabilities, offers a robust solution to this challenge. By leveraging machine learning algorithms, AI systems can analyse vast datasets to identify anomalies and predict fraudulent activities with remarkable accuracy and efficiency (Afolabi & Adeyemi, 2021).

The adoption of AI in Nigerian public organisations is particularly pertinent, given the pervasive nature of corruption and fraud in the country. According to Nwaogu and Okoli (2020), fraud in public organisations has eroded public trust and significantly hampered economic development. The implementation of AI-driven fraud detection systems can potentially transform the landscape by providing more transparent, accountable, and efficient governance. These systems not only enhance the detection of fraudulent activities but also aid in preventive measures by identifying potential risks before they materialise.

Furthermore, AI technologies facilitate continuous learning and adaptation, which is crucial in an environment where fraudsters continually devise new methods to bypass security measures. As noted by Onuoha and Opara (2019), adaptive learning algorithms enable AI systems to evolve with the changing dynamics of fraudulent activities. This capability ensures that public organisations remain one step ahead of fraudsters, thereby safeguarding public resources more effectively. The use of AI in this context aligns with global best practices and positions Nigerian public organisations to benefit from technological advancements in fraud prevention.

The economic implications of adopting AI for fraud detection in public organisations are substantial. A study by Ojo and Fapohunda (2022) highlights that the financial losses incurred from fraudulent activities can be drastically reduced through the implementation of AI technologies. By minimising fraud, public organisations can reallocate resources towards developmental projects, thereby enhancing overall economic growth. Moreover, the efficiency gains from AI adoption can lead to significant cost savings in administrative and operational processes.

Despite the promising benefits, the adoption of AI in fraud detection within Nigerian public organisations faces several challenges. These include issues related to data privacy, technological infrastructure, and the need for skilled personnel to manage and operate AI systems. Okeke and Eze (2021) emphasise the importance of addressing these challenges through robust policy frameworks and capacity-building initiatives. Ensuring data security and fostering an environment conducive to technological innovation are critical for the successful integration of AI in fraud detection.

Concept of Fraud

Any action that depends on lying to get an advantage is considered fraud. It also includes lying about the truth or withholding important information in order to persuade someone else to act negatively. Chen (2024) defined fraud as an intentional act of deceit designed to reward the perpetrator or to deny the rights of a victim. It entails lying, fabricating documents, or withholding crucial facts. On the other hand, deliberate distortion of the truth to coerce someone into giving up something of value or a legally protected right is also considered fraud. Fraud is also defined as the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organisation's resources or assets (Lin, Huang, Liao, Liu, & Zhou, 2022). Since fraud involves guilt, intentional distortion of the truth, and frequently criminal activity in act or practice, it is a recurrent problem in corporate organisations and is drawing attention from around the world.

Additionally, fraud can be roughly classified into two categories: criminal fraud (which involves theft and deception) and civil fraud (which is perpetrated when information is

purposefully or negligently misrepresented). Similarly, the motive of fraud is composed of greed, opportunity, need, and exposure [GONE] (Bologna 1992, cited by Kaiser 2017). Another definition of fraud is wrongdoing committed with the intention of gaining an unlawful benefit or violating the rights of the victim. Wolfe & Hermonson (2004) proposed the fraud diamond, which consists of pressure, opportunity, rationalisation, and capability, and Cressey (1953) proposed the fraud triangle, which consists of pressure (since it may be caused by personal issues), opportunity (where the pressure creates the motive for the crime to be committed), and rationalisation (cited by Sujeewa & Azam 2018). Furthermore, lying or using deceit to obtain money or other financial benefits is regarded as fraud since it is the intentional use of deception to do harm to another person or further one's own objectives. It usually entails speaking falsely, concealing important information, or operating without authorization. Fraud can arise from a number of situations, such as employment, identity theft, and financial transactions. Like other illegal activity, fraud is facilitated by an easy source of motivated offenders, appropriate targets, and inadequate supervision. According to Kazaara and Kazaara (2023), cited in Nakanjako and Zikusooka (2024), fraud includes manipulating, falsifying, or altering documents and records; recording transactions without substance; deliberate misapplication of accounting principles; etc., to mention a few.

Concept of Fraud Detection

The technique of spotting fraudulent attempts or behaviours is known as fraud detection. It entails the process of locating and stopping fraudulent activity in systems, transactions, data, APIs, and apps. According to Kanade (2021), fraud detection is defined as a process that detects scams and prevents fraudsters from obtaining money or property through false means. Fraud detection is the process of keeping an eye on customer behaviour and transactional patterns in order to identify and combat fraudulent activities. It frequently serves as a key component of a company's loss prevention strategy and occasionally is integrated into its larger anti-money laundering (AML) compliance procedures. A detection system must be in place to stop fraud from occurring and shield customers and companies from the potential financial losses brought on by these actions.

Furthermore, Gillis (2024) mentioned that fraud detection is a set of activities undertaken to prevent money or property from being obtained through false pretenses. Several governmental organisations use fraud detection. Kadar (2022) explained that fraud detection is an action set in place to prevent criminals from gaining monetary advantages through false pretenses. The process of employing methods and instruments to stop the theft of funds, assets, and information is known as fraud detection. It is a security barrier that guards against both felony offences and more minor transgressions as well as other types of fraud. A collection of procedures and evaluations known as fraud detection enables companies to spot and stop illegal financial activity. Moreover, Kou, Lu, Sinvongwattan, and Huang (2004), cited in Hilal, Gadsden, and Yawney (2022), mentioned that fraud detection involves identifying fraud as quickly as possible once it has been perpetrated.

Concept of Artificial Intelligence (AI)

Artificial intelligence (AI) is the idea and practice of creating computer systems that can do tasks like speech recognition, decision-making, and pattern recognition that traditionally needed human intelligence. Natural language processing, machine learning, deep learning, and other technologies are all included under the broad term artificial intelligence (AI) (NLP). Laskowski (2024) defined artificial intelligence as the simulation of human intelligence processes by

machines, especially computer systems. Expert systems, machine learning, speech recognition, and natural language processing (NLP) are a few uses of AI. Artificial Intelligence (AI) refers to the development of computer systems that can perform tasks that typically require human intelligence (Bassey and Owushi, 2023).

Furthermore, Udo-Okon and Akpan (2024) mentioned that AI is a branch of computer science called artificial intelligence studies how computers learn, comprehend data, recognize characters in images, analyses pictures, and simulate how the eyes work. In its widest definition, artificial intelligence (AI) refers to the intelligence displayed by machines, especially computer systems. This area of computer science study focuses on creating and analysing tools and software that allow machines to sense their surroundings and use intelligence and learning to make decisions that will increase their chances of accomplishing specific objectives. Copeland (2024) mentioned that the simplest human behaviour is ascribed to intelligence, while even the most complicated insect behaviour is usually not taken as an indication of intelligence. The intelligence that allows a machine or computer to copy or replicate human abilities is known as artificial intelligence, or AI. Computers and other devices can mimic human intelligence and problem-solving abilities thanks to artificial intelligence (AI) technology. The perfect feature of artificial intelligence would be its capacity for reasoning and action towards a certain objective. Kanade (2022) mentioned that artificial intelligence (AI) is the intelligence of a machine or computer that enables it to imitate or mimic human capabilities. Artificial intelligence uses clever algorithms integrated into a dynamic computing environment to mimic human thought processes.

Furthermore, Glover (2024) mentioned that artificial intelligence refers to computer systems that are capable of performing tasks traditionally associated with human intelligence, such as making predictions, identifying objects, interpreting speech, and generating natural language. AI systems pick up this skill by sifting through vast volumes of data and searching for patterns to mimic in their own decision-making. While humans will frequently oversee an AI's learning process, encouraging wise choices and punishing foolish ones, some AI systems are built to learn on their own. The goal of artificial intelligence (AI), a broad field of computer science, is to create machines that are able to carry out tasks that normally require human intelligence.

With the use of artificial intelligence, machines can now match or even surpass human mental capacity. Artificial intelligence (AI) is permeating every aspect of daily life, from the creation of self-driving cars to the spread of generative AI tools. The technological and scientific field of artificial intelligence is focused on engineering systems that produce outputs for a certain set of human-defined objectives, such as content, forecasts, recommendations, or judgements. The simulation of human intelligence in robots that are designed to think and behave like people is known as artificial intelligence, or AI. Cognitive talents include things like learning, reasoning, problem-solving, perception, and language understanding. Making a computer, a robot controlled by a computer, or a piece of software think intelligently like a human being is known as artificial intelligence. Artificial Intelligence is achieved via the examination of cognitive processes and the patterns found in the human brain.

Concept of Fraud Control

Fraud control, often known as fraud prevention, describes the procedures, roles, and policies of an organisation that prevent fraud from happening. The application of a plan to identify fraudulent transactions and stop them from harming public organisations' finances and reputation

is known as fraud control. According to Mayo and Bpp (2006), cited in Agyemang (2020), fraud control is the measure taken by public organisations for the purpose of protecting their resources against fraud, ensuring accuracy and reliability, securing compliance with organization policies, and evaluating the level of performance in the division of the organisation.

Furthermore, Dzomira (2015) explained that control of fraud needs a system of policies and procedures that, in aggregate, minimise the likelihood of fraudulent activities that may occur. The process of putting policies and processes in place to stop, identify, and deal with fraudulent activity within an organisation is known as fraud control. Building a robust internal control system is a crucial part of fraud control. This entails putting in place segregation of responsibilities, carrying out frequent audits, and upholding stringent authorization and approval procedures.

Types of Fraud in Public Organization

Fraud in public organisations encompasses various illegal activities that aim to deceive and financially benefit at the expense of the public sector. The complexity and diversity of public organisations make them susceptible to different types of fraud. Here are some common types of fraud found in public organisations (Deloitte, 2022):

Embezzlement: Embezzlement occurs when individuals entrusted with managing public funds misappropriate these funds for personal use. This type of fraud often involves manipulating financial records to hide the theft, making detection challenging. Public officials or employees may divert money from accounts or programmes, falsify receipts, or create fake vendors to syphon off funds.

Procurement Fraud: Procurement fraud involves illegal activities during the process of acquiring goods and services. This can include bid rigging, where the bidding process is manipulated to favour a particular contractor, or kickbacks, where a contractor gives a portion of the contract's value to an employee in exchange for winning the contract. Public organisations often face procurement fraud due to large-scale purchasing activities and complex supply chains.

Payroll Fraud: Payroll fraud happens when employees manipulate the payroll system to receive undue benefits. This can include ghost employees, where nonexistent employees receive salaries, or falsifying timesheets to claim overtime or additional hours not worked. Payroll fraud not only results in financial loss but also affects organisational morale and operational efficiency.

Misuse of Assets: This type of fraud involves the unauthorised use of public assets for personal gain. Examples include using government vehicles for personal errands, unauthorised use of public property, or misappropriation of resources. Such misuse often goes unnoticed if adequate controls and monitoring mechanisms are not in place.

Bribery and Corruption: Bribery and corruption are significant issues in public organizations. Officials may accept bribes to influence decisions, such as granting permits, licenses, or contracts. Corruption can undermine public trust and lead to the inefficient use of public resources. It often involves a network of individuals working together to exploit their positions for personal gain.

Financial Statement Fraud: This type of fraud involves falsifying financial statements to present a misleading picture of an organisation's financial health. Public officials may manipulate accounting records, understate liabilities, or overstate revenues to conceal financial

mismanagement or to meet budgetary requirements. Financial statement fraud can have severe implications, including incorrect allocation of public funds and loss of public confidence.

Grant Fraud: Public organisations often distribute grants to support various programmes and initiatives. Grant fraud occurs when individuals or organisations submit false information to receive grant funds or misuse the funds for unintended purposes. This type of fraud can undermine the effectiveness of public programmes and lead to significant financial losses.

Fraud Detection Strategies Using Artificial Intelligence

Artificial intelligence (AI) fraud detection works by applying machine learning algorithms that are intended to examine behaviours and identify abnormalities suggestive of fraud. Establishing a baseline of typical transaction patterns and user behaviours is the first step. After that, the algorithm keeps an eye on the data, searching for any departures from the average. The AI model adjusts its settings in response to fresh and varied data, improving its ability to distinguish between suspicious and genuine activity. The following are fraud detection strategies using artificial intelligence as mentioned by Martins (2024):

Anomaly Detection: In transactional data, anomalous patterns or departures from typical behaviour are detected using artificial intelligence systems. The algorithms identify valid transactions and highlight questionable activity suggesting possible fraud by training on past data. More precise fraud detection is made possible by artificial intelligence systems' exceptional ability to identify intricate patterns, connections between data points, and abnormalities in big datasets. Real-time transaction analysis made possible by AI enables quick action in the event of possible fraud.

Risk Scoring: Artificial intelligence assigns risk rankings to transactions or user accounts based on a variety of parameters, including transaction amount, location, frequency, and historical behaviour, using machine-learning algorithms. Elevated risk scores facilitate the allocation of resources and concentrate attention on particular transactions or accounts that require additional scrutiny. Based on a predetermined set of criteria and data points, artificial intelligence uses this analytical approach to determine the probability that a transaction or activity is fraudulent. A risk score can be assigned to any event or action, taking into account user behaviour, transaction history, and network connections. This risk score shows how likely it is that the action or event will be fraudulent. With the use of these ratings, companies are able to identify suspicious trends, follow anomalies, and decide with confidence what steps to take next to approve or deny a transaction.

Identification Verification: In order to prevent identity theft, artificial intelligence has been used by employing algorithms to examine and validate user-provided data, such as identification documents or facial recognition data.

Adaptive learning: As strategies change, machine learning can adjust to new data, keeping models current and able to identify new fraud tendencies. Adaptive learning makes use of artificial intelligence to develop and enhance its detecting skills over time. By analyzing vast amounts of transactional data, adaptive learning enables these systems to update their algorithms based on new fraud tactics, making them more resilient against evolving threats.

Fraud Detection Control Using Artificial Intelligence

Artificial intelligence (AI) has transformed fraud detection and control, helping public organisations combat fraudulent activities by offering sophisticated methods to detect, prevent, and mitigate risks. The following is how AI is utilised in fraud detection and control:

Advanced Data Analytics: AI algorithms excel in analysing large volumes of transactional and behavioural data to identify patterns indicative of fraudulent ehavior. Techniques such as machine learning, deep learning, and anomaly detection models enable organisations to detect anomalies in real-time, thereby improving fraud detection accuracy (Bhattacharyya et al., 2018).

Behavioural Biometrics: AI-powered systems can analyse unique user behaviours and biometric data to establish baseline patterns for genuine users. Deviations from these patterns can indicate potential fraud, allowing for proactive intervention before significant losses occur (Singh et al., 2020).

Network and Link Analysis: AI facilitates the analysis of complex networks and relationships between entities (such as customers, transactions, and devices) to uncover hidden connections that may signal fraudulent activities, such as organised fraud rings or money laundering schemes (Kshetri, 2020).

Real-time Decision Making: AI-driven fraud detection systems operate in real-time, enabling immediate responses to suspicious activities. These systems can autonomously block transactions, trigger alerts for further investigation, or dynamically adjust fraud prevention strategies based on emerging threats (Phua et al., 2021).

Effect of Artificial Intelligence on Fraud Detection and Control

Artificial intelligence (AI) has revolutionised fraud detection and control across various industries, offering advanced capabilities to identify and mitigate fraudulent activities. This transformation is driven by AI's ability to analyse vast amounts of data swiftly and accurately, uncovering patterns and anomalies that traditional methods might miss. The following are the effects of AI on fraud detection and control:

Improved Detection Accuracy: AI-powered algorithms can analyse historical data to identify patterns indicative of fraudulent behaviour with greater precision than rule-based systems. Machine learning models, such as neural networks and decision trees, continuously learn from new data, enhancing their ability to detect evolving fraud tactics (Abawajy, 2020).

Real-time Monitoring: AI enables real-time monitoring of transactions and activities, allowing organisations to detect fraud as it happens. This proactive approach helps minimise financial losses and prevent potential damages to both businesses and customers (Choo et al., 2020).

Reduced False Positives: AI systems can significantly reduce false positives by distinguishing between genuine transactions and suspicious activities more accurately. This capability enhances operational efficiency by minimising the need for manual review and investigation of non-fraudulent transactions (Bolton et al., 2021).

Adaptive Security Measures: AI's adaptive capabilities allow fraud detection systems to evolve alongside new fraud tactics. By continuously learning from new data and adapting to changing patterns, AI systems can maintain their effectiveness in combating fraud over time (Li et al., 2018).

Conclusion

The integration of artificial intelligence (AI) in fraud detection and control is a significant advancement in combating financial malfeasance in public organizations. AI's advanced data analytics and pattern recognition capabilities provide robust solutions for identifying anomalies and predicting fraudulent activities. In Nigeria, where corruption is pervasive, AI-driven systems can enhance transparency, accountability, and efficiency. Adaptive learning allows AI to evolve with fraud tactics, safeguarding public resources. Despite challenges like data privacy and infrastructure, strategic policy measures can facilitate successful AI adoption in fraud prevention.

Recommendations

1. Public organisations should allocate resources to acquire and maintain cutting-edge AI technologies and infrastructure. This includes high-performance computing systems, robust data management platforms, and sophisticated AI software capable of real-time data analysis and pattern recognition.
2. To effectively implement and manage AI-driven fraud detection systems, public organisations must invest in training and educating their workforce. This involves providing specialised training programmes for IT staff, data scientists, and auditors to ensure they are proficient in AI technologies and can adapt to evolving fraud tactics.
3. Public organisations should develop and enforce data governance standards to ensure the responsible use of AI technologies. This includes establishing clear guidelines for data collection, storage, and sharing, as well as implementing measures to protect sensitive information and prevent misuse of AI systems.

REFERENCES

Abawajy, J. H. (2020). *Machine Learning and Deep Learning for Fraud Detection.* IEEE Transactions on Dependable and Secure Computing.

Adedeji, T., & Abayomi, J. (2021). *Artificial Intelligence in Fraud Detection: Challenges and Opportunities in Nigeria.* Lagos: Nigerian Institute of Management.

Afolabi, O., & Adeyemi, K. (2021). *Enhancing Public Sector Accountability through AI.* Ibadan: University of Ibadan Press.

Agyemang, J. K. (2020). Internal Control and Fraud Prevention. *International Journal of Scientific Research and Management Studies*, 1(1), 1-11.

Bassey, M. M., & Owushi, E. (2023). Adoption of artificial intelligence in library and information science in the 21st century: assessing the perceived impacts and challenges by librarians in Akwa Ibom and Rivers States. *International Journal of Current Innovations in Education*, 6(1), 75-85.

Bhattacharyya, S., Chakraborty, S., & Karforma, S. (2018). Fraud Detection and Prevention using Machine Learning and Deep Learning Approaches: A Review. *International Journal of Computational Intelligence and Applications.*

Bolton, R., Hand, D. J., & Adams, N. M. (2021). When Good Models Go Bad: Managing False Positives in Fraud Prevention. *Journal of Marketing Analytics.*

Chen J. (2024) Fraud: definition, types, and consequences of fraudulent behavior available at: https://www.investopedia.com/terms/f/fraud.asp

Choo, K. K. R., Liu, C., & Liu, L. (2020). Artificial Intelligence for Cybersecurity: A Comprehensive Survey. IEEE Access.

Copeland B. (2024). Artificial Intelligence. Available at: https://www.britannica.com/technology/artificial-intelligence/Reasoning

Deloitte. (2022). "Leveraging Technology to Combat Fraud in Public Organizations." Retrieved from Deloitte.

Dzomira, S. (2015). Fraud Prevention and Detection. *Research Journal of Finance and Accounting*, 6(14), 37-43.

Gillis, A. S. (2024). Fraud Detection. Available at: https://www.techtarget.com/searchsecurity/definition/fraud-detection

Glover E. (2024) Artificial Intelligence. Available at: https://builtin.com/artificial-intelligence

Hilal, W., Gadsden, S. A., & Yawney, J. (2022). Financial fraud: a review of anomaly detection techniques and recent advances. Expert systems With applications, 193, 116429.

Kadar, T. (2022). Fraud Detection: Its Importance & How to Choose the Right System. Available at: https://seon.io/resources/fraud-detection-and-prevention/

Kaiser, S. A. (2017). Multistatic Passive Coherent Location Using the Global Positioning System. The Pennsylvania State University.

Kanade V. (2022) What Is Artificial Intelligence (AI)? Definition, Types, Goals, Challenges. Available at: https://www.spiceworks.com/tech/artificial-intelligence/articles/what-is-ai/

Kanade, V. (2021). What Is Fraud Detection? Definition, Types, Applications, and Best Practices. Available at: https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-fraud-detection/

Kshetri, N. (2020). Artificial Intelligence, Crime, and Justice: Predictive Policing, AI Surveillance, and AI Fraud Detection. *Journal of Criminal Justice and Law Review.*

Laskowski N. (2024). What is Artificial Intelligence (AI). Available at: https://www.techtarget.com/searchenterpriseai/definition/AI-Artificial-Intelligence

Li, X., Zhu, T., & Cheng, T. H. (2018). A Deep Learning Approach for Credit Card Fraud Detection. IEEE Transactions on Neural Networks and Learning Systems.

Lin, B., Huang, J., Liao, Y., Liu, S., & Zhou, H. (2022). Why do employees commit fraud? Theory, measurement, and validation. *Frontiers in psychology*, 13, 1026519. https://doi.org/10.3389/fpsyg.2022.1026519

Martins, G. (2024). Machine Learning and Artificial Intelligence in Fraud Detection. Available at: https://www.experian.co.uk/blogs/latest-thinking/guide/machine-learning-ai-fraud-detection/

Nakanjako S., Zikusooka E. (2024). Internal Auditing and Fraud Prevention in Organizations. A Case Study of Nssf Kampala Area. *Metropolitan Journal of Business & Economics,* 3(6), 358-367.

Nwaogu, E., & Okoli, C. (2020). Corruption and Fraud in Nigerian Public Organizations: The Role of AI. *Journal of African Development*, 15(3), 45-60.

Ojo, A., & Fapohunda, O. (2022). *Economic Impact of Fraud Reduction in Nigerian Public Organizations*. Abuja: National Bureau of Economic Research.

Okeke, R., & Eze, U. (2021). *Technological Infrastructure and AI Adoption in Nigeria.* Enugu: University of Nigeria Press.

Onuoha, I., & Opara, G. (2019). Adaptive Learning Algorithms for Fraud Detection in Public Organizations. *Nigerian Journal of Technology*, 28(2), 115-130.

Phua, C., Lee, V. C. S., & Smith, K. C. (2021). *Applications of Artificial Intelligence in Financial Fraud Detection and Prevention: A Systematic Review.* Expert Systems with Applications.

Singh, S., Noore, A., & Ratha, N. K. (2020). *Behavioral Biometrics for Fraud Detection: Challenges and Opportunities.* IEEE Transactions on Dependable and Secure Computing.

Sujeewa M. M. G. & Azam S.M. F. (2018). The new fraud triangle theory-Integrating ethnical values of employees. *International Journal of Business, Economics and Law.* 16(5): 52-54.

Udo-Okon, T. N. and Akpan, E. E. (2024). The Challenges of Artificial Intelligence in Library Management System. *Intercontinental Academic Journal of Library and Information Science*, 6(1), 96-107.