Enhancing Fraud Detection in Finance and Insurance: Harnessing the Power of Machine Learning and Advanced Data Analytics for Real-Time Insights

Adetola Akintola
Department of Internal Audit and Control,
Leadway Pension, PFA, Lagos
adetolaakintola29@gmail.com
DOI: 10.56201/jafm.v9.no12.2023.pg206.217

Abstract

This study did an exploration of the combination of the application of cross cutting-edge technologies in the finance and insurance sectors' financial fraud detection mechanisms to identify, analyze, and prevent fraudulent activities efficiently and effectively, thereby appealing to a global community by demonstrating the cross-industry benefits of these innovations. The paper presents a review of some critical literature on the application of machine learning and advanced data analytics for real-time insights techniques to enable the detection of financial fraud and proposes a structure for fraud detection. The systematic and comprehensive literature review of techniques applicable to enhancing fraud detection in finance and insurance fraud detection may provide a foundation to future research in this field. The adoption of the findings of Sharma and Panigrahi (2013) show the most frequently used techniques includes but not limited to Regression Models; Neural Networks; Bayesian Belief Network; Decision Trees; Naïve Bayes; Nearest Neighbour Method; Fuzzy logic, Genetic Algorithm; and Expert Systems. They all fall into the ―classification category that fundamentally makes provision for remedial measures to the prevalent challenges of financial and insurance fraud data that the research discussed. The paper recommend that the identified possibilities in technology and data-driven solutions by this study should be effectively purified to possess the ability to face the hydra-headed tact and dynamics in financial and insurance fraud against the perpetrators as they always strive to innovate in the world of advancement.

Key Words: *Data Analysis; Fraud Detection; Finance; Insurance; Machine Learning*

1. Introduction

Following an increase in financial accounting fraud in the current economic scenario experienced, Financial Accounting Fraud Detection (FAFD) has become an emerging subject of utmost importance to the academic community, financial research and development across industrial organisations in the world. The failure of internal auditing system of the organization in identifying the financial frauds has led to adoption of specialized procedures to detect finance and insurance fraud, collective known as forensic accounting. Data mining techniques are providing great aid in financial accounting fraud detection, since dealing with the large data volumes and complexities of financial data are big challenges for forensic accounting (Sharma

and Panigrahi, 2013). In addition, over the past years though developing countries are still in poverty of power supply as Audu, PAUL and Ameh (2017) highlighted, a technological revolution has occurred on the Internet that paved to the emergence of modern services especially in e-commerce and money transfer. E-commerce is one of the many economic domains in information and communications technology that contributed to business improvement, paved the way for managing medium and small companies, reducing costs and saving time, and increasing productivity. The growth in e-commerce enabled most companies and organizations to perform their financial transactions electronically through the adoption of payment systems such as Healthcare Insurance systems, Telecommunication systems, and the Financial Sector. The civil aviation sector is also greatly influenced (PAUL, 2019; PAUL et al, 2025). Lately, there is a noticeable rise in the number of financial transactions due to the large adoption of Internet bank services and financial institutions as well as e-commerce. The Internet has played an important role in making an online payment, that in return has become a breeding ground for malicious attackers to exploit these services for performing fraudulent businesses leading to the emergence of cybercrime that targets e-banking services as a result of a significant rise in the number of frauds by fraudsters causing an annual loss with an approximate cost of billions of dollars.

Financial fraud is an issue with far reaching consequences in the finance industry, government, corporate sectors, and for ordinary consumers in the post-COVID 19 economic down turn era (Orokpo and Paul, 2022; Agba et al, 2022). Increasing dependence on new technologies such as cloud and mobile computing in recent years has compounded the problem. The importance of harnessing the power of machine learning and advanced data analytics for real-time insights hinges on the fact that traditional methods involving manual detection are not only time consuming, expensive and inaccurate, but in the age of big data they are also impractical. Not surprisingly, financial institutions have turned to automated processes using statistical and computational methods (West and Bhattacharya, 2016).

Insurance fraud represents a formidable challenge for the insurance industry, leading to considerable financial losses and inflated premiums for legitimate policyholders. As fraudulent schemes become increasingly sophisticated, traditional fraud detection methods, which rely heavily on rule-based systems and manual reviews, have struggled to keep pace (Srinivasagopalan, 2022). These conventional approaches often suffer from high false positive rates, inefficiencies in processing, and a limited ability to adapt to evolving fraud tactics.

Accordingly, traditional fraud detection techniques are often characterized by their reliance on predefined criteria and static rules that can quickly become outdated. Rule-based systems, while providing a foundation for fraud detection, lack the flexibility to address the nuances of more complex fraud schemes (Srinivasagopalan, 2022). They asserted that manual reviews, although thorough, are resource-intensive and susceptible to human error, leading to delays and inconsistencies in identifying fraudulent claims. Notwithstanding the above, Al-Hashedi and Magalingam (2021) identified different types of financial frauds to include credit card fraud, mortgage fraud, money laundering, financial statement fraud, securities and commodities fraud, insurance fraud, and cryptocurrency fraud.

This paper dealt with an introduction of financial fraud and the emergence of fraudulent act in critical sectors like finance, insurance and cybercrime that aims at financial services thereby causing a substantial rise in annual loss with an estimated cost of billions of dollars. It also sees a review of challenges facing fraud detection in finance and insurance; the effects of fraud on finance and insurance; the impact of the optimization of machine learning models and advanced data analytics; suggestion for further studies, and concluding remarks with recommendations

2. A Review of Challenges Facing Fraud Detection in Finance

Fraud detection has been studied by researchers and scientists in various surveys and review articles that have emerged in academic publications. Abdallah, Maarof, and Zainal (2016) says, nowadays, most organizations, companies and government agencies have adopted electronic commerce to increase their productivity or efficiency in trading products or services; in areas such as credit card, telecommunication, healthcare insurance, automobile insurance, online auction, etc. (Allen, 2000, Bolton and Hand, 2001, Philip and Sherly, 2012). Electronic commerce systems are used by both legitimate users and fraudsters; hence they become more vulnerable to large scale and systematic fraud. Fraud is a crime where the purpose is to appropriate money by illegal means. The Association of Certified Fraud Examiners (ACFE) defines “fraud” as: the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets (ACFE, 2002). Internet Crime Complaint Centre (IC3) is a valuable resource for both victims of Internet crime and law enforcement agencies in identifying, investigating and prosecuting these crimes.

Al-Hashedi and Magalingam (2021) maintains that financial fraud is an essential problem that affects both the finance sector and everyday life and plays a critical role in influencing integrities and confidences in financial sectors as well as the individuals’ cost of living. Financial fraud is known as financial abuse which is a big concern in economic society causing huge losses to the economy of governments, organizations, corporate sectors or even individuals. It can be defined as an act of wrongful or illegal behavior, resulting in a beneficial gain to either individual or organization from unethical and illegal ways. Fraud detection techniques were introduced to identify abnormal activities that occurred in past transactions aiming to discover cases that fraudsters intend to violate the values that the organizations make in exchange for supplying services. Various methods have been proposed to detect fraud, but these methods are infeasible due to the constant evolution of new methods developed by fraudsters or in new technologies such as cryptocurrency. According to the fact that any E-commerce system that involves online transactions such as financial services is vulnerable to be compromised by fraudsters. Therefore, anti-fraud has become a topic of interest by many scientists to explore the issues related to this field. The important issues of fraud motivated scientists to develop detection methods or even estimate fraud risk.

According to Abdallah, Maarof, and Zainal (2016), fraud detection is a complex domain; we may find that a fraud detection system is prone to fail, has a low accuracy rate, or gives many false alarms. It is extremely difficult for electronic commerce systems to handle fraud problem forcing them to incur heavy losses. This happens because fraud detection systems need to deal

with multiple challenges to be taken into account.

3. The Effects of Fraud on Finance and Insurance

> In 2014, the IC3 received 269,422 complaints with an adjusted dollar loss of $800,492,073; which is a 2.39 percent increase in reported losses since 2013 ($781,841,611) (IC3, 2014). The number of complaints received by the IC3 between 2011 and 2014 and the corresponding dollar losses. The amount of loss steadily increase while number of complaints decrease; this is because, fraud is causing more loss now compared to the past. These huge numbers of losses have increased the importance of fraud fighting (Kou et al., 2004; Abdallah, Maarof, and Zainal, 2016).

West and Bhattacharya (2016) Financial fraud is a broad term with various potential meanings, but for this purposes it can be defined as the intentional use of illegal methods or practices for the purpose of obtaining financial gain (Zhou and Kapoor, 2011). Fraud has a large negative impact on business and society: credit card fraud alone accounts for billions of dollars of lost revenue each year (Bhattacharyya et al., 2011), and some figures suggest that the total yearly cost to the US could be in excess of $400 billion (Kirkos et al., 2007), while a third study shows that UK insurers are out 1.6 billion pounds a year due to fraudulent claims (Ngai et al., 2011). Financial fraud also has broader ramifications on the industry, such as providing funding for illicit activities like drug trafficking and organised crime (Bhattacharyya et al., 2011). For credit card fraud the cost is typically worn by the merchants, who end up paying shipping, chargeback, and administrative costs as well as losing consumer confidence after being victim to a fraudulent transaction. In this way, we can see the widespread consequences that fraud can have and the importance in minimizing it.

Advancements in modern technologies such as the internet and mobile computing have led to an increase in financial fraud in recent years. Social factors such as the increased distribution of credit cards has not only increased spending but also resulted in an increase to fraud. Fraudsters are continually refining their methods, and as such there is a requirement for detection methods to be able to evolve accordingly (Bhattacharyya et al., 2011). Data mining has already been shown to be useful in similar domains such as credit card approval, bankruptcy prediction, and analysis of share markets. Fraud detection is considered to be a similar classification problem but with a vast imbalance in fraudulent to legitimate transactions, and a sizeable difference in cost for misclassifying them (Duman and Ozcelik, 2011). Data mining approaches are also applicable to fraud detection for their efficiency at processing large datasets and their ability to work without requiring knowledge of the input variables (Ravisankar et al., 2011).

A useful framework for applying data mining to fraud detection is to use it as a method for classifying suspicious transactions or samples for further consideration. Studies show that reviewing 2% of credit card transactions could reduce fraud losses to 1% of the total cost of all purchases, with more assessments resulting in smaller loss but with an increase in auditing costs (Quah and Sriganesh, 2008). A multi-layer pipeline approach can be used with each step applying a more rigorous method to detect fraud. Data mining can be utilized to efficiently filter

out more obvious fraud cases in the initial levels and leave the more subtle ones to be reviewed manually (Quah and Sriganesh, 2008).

4. The Impact of the Optimization of Machine Learning Models and Advanced Data Analytics

> The detection of [financial] fraud using traditional internal audit procedures is a difficult or sometimes an impossible task. First, the auditors usually lack the required knowledge concerning the characteristics of accounting fraud. Second, as the fraudulent manipulation of accounting data is so infrequent, most of the auditors lack the experience and expertise needed to detect and prevent frauds. Finally, the other concern people of finance department like Chief Financial Officer (CFO), financial managers and accountants are intentionally trying to deceive the internal or external auditors. While knowing the limitations of an audit, finance and accounting managers have concluded that traditional and standard auditing procedures are insufficient to detect frauds (Sharma and Panigrahi, 2013).

These limitations of financial auditing suggest the need for additional automatic data analysis procedures and tools for the effective detection of falsified financial statements.

Financial fraud is an issue that has wide reaching consequences in both the financial industry, insurance and daily life. According to West and Bhattacharya (2016), fraud reduces confidence in industry, destabilize economies, and affect people's cost of living. Traditional approaches relied on manual techniques such as auditing, which are inefficient and unreliable due to the difficulty of the problem. Data mining-based approaches have been shown to be useful because of their ability to identify small anomalies in large data sets. There are many different types of fraud, as well as a variety of data mining methods, and research is continually being undertaken to find the best approach for each case.

The purpose of fraud prevention mechanism is to protect the technological systems against fraud by stopping fraud from occurring in the first place. Nevertheless, this mechanism alone is not enough to halt fraud (Abdallah, Maarof and Zainal, 2016). Fraud detection is also proposed to improve the technological systems security. Fraud detection detects and recognizes fraudulent activities as they enter the systems and reports them to a system administrator. Similar to detection approaches in Intrusion detection system (IDS), FDS also uses misuse and anomaly based approaches to detect fraud. Both misuse based FDSs and anomaly based FDSs utilize data mining techniques to determine fraud from large amount of incoming data stream. However, there are issues and challenges that hinder the development of an ideal FDS for E-commerce system; such as concept drift, supports real time detection, earliness of detection, skewed distribution, large amount of data, misclassification cost, etc. The presence of any one of these challenges will lead to high false alerts, low detection accuracy and slow detection. These are the parameters used to characterize the performance of FDS.

The study focuses on optimizing various machine learning (ML) models to enhance fraud detection. The insurance company aims to improve the performance of several ML models, including Isolation Forest, weighted logistic regression, Random Forest Classifier, Support Vector Machine (SVM), K-Nearest Neighbors (KNN), and XGBoost (Srinivasagopalan, 2022). The objective is to compare these models and identify strategies for enhancing their effectiveness in detecting fraudulent claims. The methodology begins with the collection of relevant datasets that contain information on insurance claims and associated fraud indicators. The datasets are used to train the selected ML models, ensuring that each model is exposed to a diverse range of fraud scenarios. Model training involves fine-tuning hyper-parameters and adjusting algorithms to improve performance.

Performance evaluation therefore is a key aspect of this study. Metrics such as precision, recall, F1-score, and AUC-ROC are used to assess the effectiveness of each ML model in identifying fraudulent claims. The study also involves optimizing the models by employing techniques such as feature selection, parameter tuning, and cross-validation to enhance their performance.

The results of the study demonstrate notable improvements in model performance. Each ML model shows enhanced accuracy in detecting fraudulent claims, with reduced false positive rates compared to baseline models. The optimization process reveals that models such as Random Forest Classifier and XGBoost provide superior performance, offering a balance between high detection accuracy and manageable false positive rates. The study concludes that optimizing ML models through advanced techniques significantly enhances fraud detection capabilities, making them valuable tools for the insurance company (Srinivasagopalan, 2022).

From the foregoing, Al-Hashedi and Magalingam (2021) maintained that data mining is an approach used in extracting meaningful data from a given dataset using one or more approaches such as statistical, machine learning, mathematical or artificial intelligence techniques. Among these approaches, different kinds of techniques can be applied for financial fraud such as Naïve Bayes (NB), support vector machine (SVM), Logistic Regression (LR), and many more [11]. Generally, data mining is usually used to discover financial frauds that can be classified into six categories such as classification, visualization, outlier detection, clustering, regression, and prediction [4]. Furthermore, it is believed that the last two years have witnessed a large operation of fraud activities targeting 1 out of 3 organizations. But the most unexpected thing is that only 10% of these financial frauds are discovered by chance [14]. Several studies have been conducted on the annual cost of financial fraud in the U.S. and the U.K. Moreover, the figures of these studies show that financial fraud in the U.S. made a loss of $400 billion every year while 1.6 billion pounds to insurers in the United Kingdom. Moreover, A study estimates that fraud activities will be increased especially in online fraud from $10.7 billion in 2015 to $25.6 billion in 2020 [15]. Besides that, financial fraud also has tremendous consequences on society, which can be used for supplying illegal activities such as organized crime and fund terrorism [16]. However, most organizations are interested to take action against fraudulent activities.

Thus, to determine the main algorithms used for financial accounting fraud detection, we present a Review of data mining techniques identified in literature applied to the detection of financial fraud. The most frequently used techniques are logistic models, neural networks, the Bayesian

belief network, and decision trees, all of which fall into the — classification category. Considering the view of Sharma and Panigrahi (2013), these techniques are discussed in more detail in the following paragraphs.

i. **Regression Models -** The regression-based models are mostly used in financial accounting fraud detection. The majority of them are based on logistic regression, stepwise-logistic regression, multi criteria decision-making method and exponential generalized beta two (EGB2). Logistic model is a generalized linear model that is used for binomial regression in which the predictor variables can be either numerical or categorical. It is principally used to solve problems caused by insurance and corporate fraud.

ii. **Neural Networks –** The neural networks are nonlinear statistical data modeling tools that are inspired by the functionality of the human brain using a set of interconnected nodes. Neural networks are widely applied in classification and clustering, and its advantages are as follows. First, it is adaptive; second, it can generate robust models; and third, the classification process can be modified if new training weights are set. Neural networks are chiefly applied to credit card, automobile insurance and corporate fraud.

iii. **Bayesian Belief Network -** The Bayesian belief network (BBN) represents a set of random variables and their conditional independencies using a directed acyclic graph (DAG), in which nodes represent random variables and missing edges encode conditional independencies between the variables. The Bayesian belief network is used in developing models for credit card, automobile insurance, and corporate fraud detection. The Bayesian belief network model correctly classified 90.3% of the validation sample for fraud detection. Bayesian belief network outperformed neural network and decision tree methods and achieved outstanding classification accuracy.

iv. **Decision Trees –** A decision tree (DT) is a tree structured decision support tool, where each node represents a test on an attribute and each branch represents possible consequences. In this way, the predictive model attempts to divide observations into mutually exclusive subgroups and is used for data mining and machine learning tasks. Decision trees are predictive decision support tools that create mapping from observations to possible consequences. These trees can be planted via machine-learning-based algorithms such as the ID3, CART and C4.5. Predictions are represented by leaves and the conjunctions of features by branches. Decision trees are commonly used in credit card, automobile insurance, and corporate fraud. To identify and predict the impact of fraudulent financial statements, classification and regression trees (CART) algorithm is introduced.

v. **Naïve Bayes -** Naïve Bayes is adopted as simple probabilistic classifier based on Bayes conditional probability rule. Naïve Bayes follows strong (naive) statistical independence assumptions for the predictor variables. It is an effective classification tool that is easy to interpret and particularly suited when the dimensionality of the inputs is high. Naïve Bayes classifier outperformed the conventional classifier. The efficiency of predicting financial fraud data was higher with no false positives with relatively low false negatives. Naïve Bayes methods are widely used in banking and financial fraud detection and claim fraud detection. To apply Ada Boosted Naïve Bayes scoring to insurance claims fraud, a case

study is given to diagnosis claim fraud.

vi. **Nearest Neighbour Method –** Nearest neighbour method is a similarity based classification approach. Based on a combination of the classes of the most similar k record(s), every record is classified. Sometimes this method is also known as the k-nearest neighbour technique. K-nearest neighbour method is used in automobile insurance claims fraud detection [46] and for identifying defaults of credit card clients.

vii. **Fuzzy logic and Genetic Algorithm –** Genetic algorithms are used in classifier systems to represent and modeling the auditor decision behavior in a fraud setting. Genetic algorithm along with binary support vector system (BSVS) which is based on the support vectors in support vector machines (SVM) are used to solve problems of credit card fraud that had not been well identified. Fuzzy Logic is a mathematical technique that classifies subjective reasoning and assigns data to a particular group, or cluster, based on the degree of possibility the data has of being in that group.

viii. **Expert Systems –** Researchers in the field of Expert systems have examined the role of Expert Systems in increasing the detecting ability of auditors and statement users. By using expert system, they could have better detecting abilities to accounting fraud risk under different context and level and enable auditors give much reliable auditing suggestions through rational auditing procedure. The research has confirmed that the use of an expert system enhanced the auditors' performance. With assistance from expert system, the auditors discriminated better, among situations with different levels of management fraud-risk. Expert System aided in decision making regarding appropriate audit actions.

As Abdallah, Maarof, and Zainal (2016) asserted, the purpose of fraud prevention mechanism is to protect the technological systems against fraud by stopping fraud from occurring in the first place. Nevertheless, this mechanism alone is not enough to halt fraud. Fraud detection is also proposed to improve the technological systems security. Fraud detection detects and recognizes fraudulent activities as they enter the systems and reports them to a system administrator (Behdad et al., 2012). Similar to detection approaches in Intrusion detection system (IDS), FDS also uses misuse and anomaly based approaches to detect fraud (Ferreira et al., 2007, Seeja and Zareapoor, 2014). Both misuse based FDSs and anomaly based FDSs utilize data mining techniques to determine fraud from large amount of incoming data stream (Ngai et al., 2011). For instance;

> In the U.S., the rapid expansion of mobile insurance has also created an environment of opportunity and challenge around fraud prevention and recovery. With the ever-increasing sector, fraud in the market can be fought using technological advancements like artificial intelligence (AI), machine learning and blockchain; these help in real time data analysis, pattern recognition and secure transactions. These innovations must however, always be perfected to remain one-step ahead of the game and always evolving in fraudulent tactics (Bokka, 2025).

Therefore, preventing fraud and providing recovery capabilities is essential to financial stability,

initiatives in trust for users, and integrity in the mobile insurance arena. By taking a proactive approach, we help everyone maintain a healthier and a more secure industry (Bokka, 2025).

Figure 1: The Impact of Insurance Fraud on Businesses and Consumers

Source: Bokka (2025).

In the submission of Bokka (2025), the impact of financial fraud is represented in the figure above.

5. Suggestion for Further Studies

Although the limitation of this study suggests that using only financial statements data may not be sufficient for detections of fraud, the significance of the optimization of machine learning models and advanced data analytics techniques in the detection of financial and insurance fraud have been acknowledged. Hence, the further studies is called for a comprehensive classification framework or a systematic review of the optimization of machine learning models and advanced data analytics application in financial and insurance fraud detection.

6. Concluding Remarks and Recommendations

> The mobile insurance space itself is a unique one, and is very much in constant movement technologically as well as in the environment in which it operates, namely a more and more digital world, and is therefore a target for fraudsters. As a result, there has been a strong need to build robust fraud prevention and recovery strategies to protect insurers and consumers alike. Artificial intelligence, machine learning and even blockchain emerge as strong tools to detect and prevent fraud. With these innovations, insurers can quickly learn about large volumes of data in real time, spot suspicious activity, and lower the chances of a financial loss (Bokka, 2025).

This paper showed an extensive review of academic articles and provide a comprehensive study and classification framework for the applications of the optimization of machine learning models and advanced data analytics to Financial and insurance fraud detection. The purpose is to inform researchers and practitioners communities of the areas in which specific data mining techniques can be applied to machine learning models and advanced data analytics to financial and

insurance fraud detection, and to report and compile a systematic review of the burgeoning works on financial and insurance fraud detection. Although this research cannot be entitled to be in-depth, we believe that it has proved a useful resource for anyone interested in financial and insurance fraud detection study, and will help simulate advance interest in the field.

On a final analysis and recommendation, the identified possibilities in technology and data-driven solutions by this study should be effectively and efficiently purified; and considered to possess the ability to face the hydra-headed and tactful dynamics in financial and insurance fraud with the perpetrators as they always strive to innovate in the world of advancement.

References

Abdallah, A., Maarof, M. A., & Zainal, A. (2016). Fraud detection system: A survey. *Journal of Network and Computer Applications*, *68*, 90-113.

Adoji, V. A., PAUL, S. O., & EDINO, F. O. (2020). Corporate social responsibility as strategic management and community development tool by Zenith Bank PLC, Nigeria. *International Journal of Management*, *11*(10), 1578-1592.

Adoji, V. A., & Paul, S. O. (2021). Middle Level Supervisors and Knowledge Sharing in Organisations: A Review. *Academia Letters*, 2.

Agba, M. S. et al (2022). COVID-19 and the workplace of higher educational institutions in developing market economies: Lessons, policy options and the emerging new normal [Special issue]. *Corporate & Business Strategy Review*, *3*(2), 328-338.

Al-Hashedi, K. G., & Magalingam, P. (2021). Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019. *Computer Science Review*, *40*, 100402.

Audu, E., Paul, S. O., & Ameh, A. (2017). Privitisation of power sector and poverty of power supply in Nigeria: A policy analysis. *International Journal of Development and Sustainability*, *6*(10), 1218-1231

Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. *Decision support systems*, *50*(3), 602-613.

Bokka, V. V. R. M. (2025). Crafting a comprehensive strategy to prevent fraud and enable recovery in mobile insurance in the USA.

Duman, E., & Ozcelik, M. H. (2011). Detecting credit card fraud by genetic algorithm and scatter search. *Expert Systems with Applications*, *38*(10), 13057-13063.

Ferreira, S. C., Bruns, R. E., Ferreira, H. S., Matos, G. D., David, J. M., Brandão, G. C., ... & Dos Santos, W. N. L. (2007). Box-Behnken design: an alternative for the optimization of analytical methods. *Analytica chimica acta*, *597*(2), 179-186.

Kirkos, E., Spathis, C., & Manolopoulos, Y. (2007). Data mining techniques for the detection of fraudulent financial statements. *Expert systems with applications*, *32*(4), 995-1003.

Kou, Y., Lu, C. T., Sirwongwattana, S., & Huang, Y. P. (2004, March). Survey of fraud detection techniques. In *IEEE international conference on networking, sensing and control, 2004* (Vol. 2, pp. 749-754). IEEE.

Ngai, E. W., Chau, D. C., & Chan, T. L. A. (2011). Information technology, operational, and management competencies for supply chain agility: Findings from case studies. *The Journal of Strategic Information Systems*, *20*(3), 232-249.

Ojonemi, P. S., Enejoh, W., Olatunmibi, O., & Enejoh, A. (2013). Examination malpractice: Challenges to human resource development in Nigeria. *International journal of capacity building in education and management*, *2*(1), 91-101.

Ojonemi, P. S., & Ogwu, S. O. (2013). Rural development policies and the challenges of realizing the millennium development goals in Nigeria. *Mediterranean Journal of Social Sciences*, *4*(2), 643-648.

Omisore, O., Eri, K., & Paul, S. O. (2014). Federal Airports Authority of Nigeria (FAAN): A chronological description of its functionality in the aviation industry. *Journal of Good Governance and Sustainable Development in Africa*, *2*(2), 193-202.

Onechojon, U. T., Ojonemi, P. S., & Mark, O. (2013). Green Audit and Environmental Sustainability in Nigeria: Unveiling Corporate Perspectives. *International Journal of Public Administration and Management Research*, *2*(1), 101-111.

Orokpo Ogbole F. E., PAUL, S. O. (2022). ICT in post Covid-19: exploring the new normal for achievement of sustainable development goals in Nigeria. International Science Journal of Management, Economics & Finance. 1(5), 46-54. doi: 10.46299/j.isjmef.20220105.06.

Paul, S. O., Enojoh, A., Omisore, O., & Enejoh, W. (2014). Deficit in Religious Practice in Nigeria: Implications for National Development. *Developing Country Studies*, *4*(4).

Paul, S. O. (2019). National urban development policy and the unanswered development question of slum in Nigeria. *International Journal of Public Policy and Administration Research*, *6*(2), 102-115.

PAUL, S O. (2019). National Civil Aviation Development Strategy and Scio-Economic Growth in Nigeria. International Journal of Social Sciences and Humanities Reviews Vol.9 No.1, January 2019; p.159 – 171.

Paul, S. O., & Chikelue, O. (2020). The inclusive and sustainable industrial development policy: which way for Nigeria? *Scientific Papers of the Legislation Institute of the Verkhovna Rada of Ukraine*, (4), 157-169.

Paul, S. O., Yakubu, A., & Apeh, G. I. (2020). Obasanjo's administration anti-corruption campaign in Nigeria and salient governance implications. *Journal DOI*, *6*(10).

PAUL, S. O., & Ofuebe, C. (2020). Unabated corruption in the government of Nigeria despite the Economic and Financial Crimes Commission: Who Bells the Cat? *Society & Sustainability*, *2*(2), 45-58.

Paul, S. O., & Ofuebe, C. (2021). Nigerian Industrialisation Challenges and Dearth of

Galvanization amidst the United Nations Industrial Development Support. *Journal of International Cooperation and Development*, *4*(1), 80-80.

Paul, S. O., & Adoji, V. A. (2022). GDP as Development Indicator and the Challenges of Actualising SDG 8: Inclusive and Sustainable Economic Growth. *Journal of International Cooperation and Development*, *5*(3), 62.

Paul, S. O., & Adoji, V. A. (2022). GDP as Development Indicator and the Challenges of Actualising SDG 8: Inclusive and Sustainable Economic Growth. *Journal of International Cooperation and Development*, *5*(3), 62.

PAUL, S. O., & Ofuebe, C. (2024). The Value Addition of National Civil Aviation Policy Implementation to Airport Development in Nigeria: A Qualitative Assessment. *International Journal of Aviation, Aeronautics, and Aerospace*, *11*(3), 1.

PAUL, S. O., Okolie, C. A., & Nnamdi-Chiawa, C. R. (2025). The emergence of civil aviation as critical public sector in Nigeria: an industry from grass to grace. *International Science Journal of Management, Economics & Finance*, *4*(1), 9-22.

Quah, J. T., & Sriganesh, M. (2008). Real-time credit card fraud detection using computational intelligence. *Expert systems with applications*, *35*(4), 1721-1732.

Ravisankar, P., Ravi, V., Rao, G. R., & Bose, I. (2011). Detection of financial statement fraud and feature selection using data mining techniques. *Decision support systems*, *50*(2), 491-500.

Salisu, O. P., & Ofuebe, O. (2019). Aviation Roadmap and development of airports in Nigeria. *Journal of Good Governance and Sustainable Development in Africa*, *5*(1), 1-24.

Salisu, P. O. (2022). Unemployment, poverty and governance questions in Nigeria: Human capital development and partnership approach options.

Seeja, K. R., & Zareapoor, M. (2014). Fraudminer: A novel credit card fraud detection model based on frequent itemset mining. *The Scientific World Journal*, *2014*(1), 252797.

Sharma, A., & Panigrahi, P. K. (2013). A review of financial accounting fraud detection based on data mining techniques. *arXiv preprint arXiv:1309.3944*.

Srinivasagopalan, L. N. (2022). AI-enhanced fraud detection in healthcare insurance: A novel approach to combatting financial losses through advanced machine learning models. *European Journal of Advances in Engineering and Technology*, *9*(8), 82-91.

West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: a comprehensive review. *Computers & security*, *57*, 47-66.

Zhou, W., & Kapoor, G. (2011). Detecting evolutionary financial statement fraud. *Decision support systems*, *50*(3), 570-575.