World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Utilizing machine learning algorithms to prevent financial fraud and ensure transaction security

Shadrack Obeng [1,*], Toluwalase Vanessa Iyelolu [2], Adetola Adewale Akinsulire [3] and Courage Idemudia [4]

[1] *KPMG, USA.*
[2] *Financial analyst, Texas, USA.*
[3] *Independent Researcher, Lagos, Nigeria.*
[4] *Independent Researcher, London, ON, Canada.*

World Journal of Advanced Research and Reviews, 2024, 23(01), 1972–1980

Publication history: Received on 08 June 2024; revised on 18 July 2024; accepted on 20 July 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.23.1.2185

Abstract

Financial fraud poses a significant threat to the global economy, necessitating advanced measures for detection and prevention. This paper explores the application of machine learning techniques to enhance transaction security and combat financial fraud. It provides a comprehensive overview of machine learning algorithms, including supervised and unsupervised learning, neural networks, and anomaly detection. Each technique's application in identifying and preventing fraudulent activities is discussed, along with their advantages and limitations. Challenges in implementing machine learning for fraud detection, such as data quality, scalability, real-time processing, and model interpretability, are examined. Ethical and privacy concerns associated with using machine learning in financial transactions are also addressed. By highlighting these aspects, the paper aims to contribute to developing more effective and ethical machine learning-based fraud detection systems, ensuring robust transaction security and fostering trust in financial institutions.

Keywords: Financial fraud; Machine learning; Transaction security; Fraud detection; Ethical concerns

1. Introduction

Financial fraud, encompassing a broad range of illicit activities such as identity theft, credit card fraud, and money laundering, represents a significant and growing threat to the global economy. The impact of financial fraud is profound, leading to substantial monetary losses for individuals, businesses, and financial institutions. According to the Association of Certified Fraud Examiners, businesses lose an estimated 5% of their annual revenues to fraud, translating to trillion dollars in global financial losses yearly (Hilal, Gadsden, & Yawney, 2022). Beyond direct financial harm, fraud erodes trust in financial systems, complicates regulatory compliance, and incurs significant costs related to fraud detection and prevention efforts (Mahtani, 2022).

The importance of transaction security within financial systems cannot be overstated. Secure transactions are the backbone of trust and efficiency in financial markets. Without robust security measures, financial systems become vulnerable to exploitation, leading to loss of consumer confidence, legal penalties, and reputational damage (Bhatia, Shukla, Punhani, & Dubey, 2021). Transaction security encompasses various strategies and technologies designed to protect sensitive financial data from unauthorized access and ensure transaction integrity and confidentiality. The rise of digital banking and e-commerce has made transaction security even more critical, as sophisticated cybercriminals often target these platforms (Albshaier, Almarri, & Hafizur Rahman, 2024).

* Corresponding author: Shadrack Obeng

In this context, machine learning has emerged as a powerful tool in the fight against financial fraud. Machine learning algorithms are designed to identify patterns and anomalies in large datasets, making them well-suited for detecting fraudulent activities that might evade traditional rule-based systems. By leveraging historical transaction data, machine learning models can learn to recognize the characteristics of legitimate and fraudulent transactions, enabling real-time detection and prevention of fraud. The adaptability of machine learning algorithms allows them to evolve with changing fraud tactics, providing a dynamic and robust defense against financial crime.

The objectives of this paper are fourfold. First, it aims to provide a comprehensive overview of the various types of financial fraud and their impact on the economy. Second, it seeks to underscore the critical importance of transaction security in maintaining the integrity and trustworthiness of financial systems. Third, the paper will explore the application of different machine learning techniques in detecting and preventing financial fraud, highlighting their effectiveness and limitations. Finally, it will discuss the challenges and future directions in integrating machine learning within financial systems, proposing potential solutions and areas for further research.

2. Background

2.1. Financial Fraud: Types and Common Techniques Used by Fraudsters

Financial fraud encompasses deceptive practices aimed at unlawfully obtaining money or assets from individuals, businesses, or financial institutions. Some of the most common types of financial fraud include identity theft, where fraudsters use stolen personal information to open accounts or make purchases; credit card fraud, involving unauthorized use of credit card information; and money laundering, where illicitly obtained money is processed to appear legitimate (Nakitende, Rafay, & Waseem, 2024). Other types include investment fraud, such as Ponzi schemes and insider trading, and cyber fraud, including phishing and malware attacks. Each type of fraud employs various techniques to deceive victims and evade detection, making financial fraud a complex and multifaceted problem (Scheaf & Wood, 2022).

Fraudsters often use sophisticated methods to carry out their schemes. For instance, in identity theft, they may employ social engineering techniques to trick individuals into divulging personal information or use data breaches to access sensitive data. Credit card fraud can involve skimming devices to capture information or creating counterfeit cards. Money laundering typically involves a series of transactions designed to obscure the origin of funds, often using shell companies and offshore accounts (Villányi, 2021). Conversely, cyber fraud leverages advanced technologies like phishing emails and malicious software to gain unauthorized access to financial systems. These techniques are constantly evolving, posing significant challenges to detection and prevention efforts (Antoniadi et al., 2021; Pomerleau & Lowery, 2020).

Traditionally, financial institutions have relied on various transaction security measures to combat fraud. Encryption is one of the most fundamental methods to protect sensitive data during transmission and storage. Two-factor authentication (2FA) adds a layer of security by requiring users to provide two forms of identification before accessing accounts (Kaur, Kaur, & Shabaz, 2022). Firewalls and intrusion detection systems (IDS) help to protect networks from unauthorized access and monitor for suspicious activities. Additionally, transaction monitoring systems use predefined rules to flag unusual or potentially fraudulent transactions for further investigation. While these measures are essential, they often fall short of keeping up with the sophisticated tactics employed by modern fraudsters (Nwaimo, Adegbola, & Adegbola, 2024; Nwaimo, Adegbola, Adegbola, & Adeusi, 2024; Oriji, Shonibare, Daraojimba, Abitoye, & Daraojimba, 2023).

2.2. Machine Learning: Basic Concepts and Types of Algorithms

Machine learning offers a promising solution to enhance transaction security and fraud detection capabilities (Trivedi, Simaiya, Lilhore, & Sharma, 2020). At its core, machine learning involves training algorithms on large datasets to identify patterns and make predictions. Supervised learning, one of the most common types of machine learning, uses labeled data to teach the algorithm what constitutes fraudulent and non-fraudulent transactions. Examples of supervised learning algorithms include decision trees, random forests, and support vector machines. Unsupervised learning, in contrast, works with unlabeled data to find hidden patterns or anomalies (Usmani, Happonen, & Watada, 2022). Clustering and anomaly detection algorithms are typical examples of unsupervised learning. Another powerful category is deep learning, which involves neural networks with multiple layers that can model complex relationships in the data (Albshaier et al., 2024; Sarker, 2021). These algorithms can adapt and improve over time, making them highly effective in identifying new and evolving fraud tactics.

The use of technology in financial fraud detection has a rich history, evolving in response to the increasing sophistication of fraud schemes. Initially, fraud detection relied heavily on manual processes and rule-based systems. Human analysts would review flagged transactions based on predefined rules, such as large transactions or those from unusual locations (Bolton & Hand, 2002). While this approach was effective to an extent, it was labor-intensive. It often resulted in high false-positive rates, causing inconvenience to legitimate customers. With more advanced computing technologies, financial institutions began incorporating statistical methods and data mining techniques into their fraud detection strategies. These methods allowed for more automated and efficient transaction data processing, though they still relied on predefined rules and thresholds. The major shift occurred with the introduction of machine learning in the early 2000s (Xu, Zhou, Sekula, & Ding, 2021). Machine learning brought the ability to analyze vast amounts of data and detect subtle patterns indicative of fraud that rule-based systems might miss. Early implementations focused on supervised learning algorithms that could be trained on historical transaction data to identify fraudulent activity (Ilori, Nwosu, & Naiho, 2024; Nwobodo, Nwaimo, & Adegbola, 2024; Nwosu & Ilori, 2024).

Over time, as fraudsters adapted to these measures, financial institutions started adopting more sophisticated machine learning techniques, including unsupervised learning and deep learning. These techniques allowed for the detection of previously unknown fraud patterns and improved the accuracy of fraud detection systems (Hilal et al., 2022; Nicholls, Kuppa, & Le-Khac, 2021). Today, machine learning is an integral part of the fraud detection arsenal for many financial institutions, offering a dynamic and robust approach to safeguarding transaction security.

In conclusion, financial fraud remains a significant threat to the global economy, with fraudsters employing increasingly sophisticated techniques to exploit vulnerabilities in financial systems. Traditional transaction security measures, while essential, often struggle to keep pace with these evolving threats. With its ability to analyze large datasets and adapt to new patterns, machine learning offers a powerful tool for enhancing fraud detection and prevention efforts. The historical progression from manual and rule-based systems to advanced machine learning algorithms underscores the ongoing evolution in the fight against financial fraud, highlighting the need for continuous innovation and adaptation in transaction security measures.

3. Machine Learning Techniques for Fraud Detection

Machine learning has revolutionized fraud detection in financial systems by leveraging large datasets to identify patterns indicative of fraudulent activity. Various machine learning algorithms play critical roles in this domain, including supervised learning, unsupervised learning, neural networks, and anomaly detection. Each technique offers unique strengths and challenges, making them suitable for different aspects of fraud detection.

3.1. Supervised Learning Algorithms

Supervised learning is one of the most widely used approaches in fraud detection. This technique involves training a model on a labeled dataset, where the input data is paired with the correct output. The goal is to learn a mapping from inputs to outputs that can be used to make predictions on new, unseen data. Common supervised learning algorithms include decision trees, random forests, support vector machines (SVM), and logistic regression (Carcillo et al., 2021; Niu, Wang, & Yang, 2019).

- Decision Trees and Random Forests: Decision trees are simple yet powerful tools that split the data into subsets based on feature values, creating a tree-like model of decisions. Random forests enhance decision trees by creating an ensemble of trees and aggregating their predictions to improve accuracy and reduce overfitting. These methods are highly interpretable and can handle both numerical and categorical data (Bhargava, Sharma, Bhargava, & Mathuria, 2013).
- Support Vector Machines (SVM): SVMs work by finding the hyperplane that best separates the data into different classes. They are effective in high-dimensional spaces and can handle non-linear relationships using kernel functions. However, SVMs can be computationally intensive and may require significant tuning (Hussain, 2019).
- Logistic Regression: Logistic regression is a statistical model that uses a logistic function to model binary dependent variables. It is straightforward to implement and interpret, making it a popular choice for binary classification problems like fraud detection (Bangdiwala, 2018).

3.2. Unsupervised Learning Algorithms

Unsupervised learning deals with unlabeled data and aims to identify hidden patterns or intrinsic structures within the data. This is particularly useful in detecting new or previously unknown types of fraud. Common unsupervised learning techniques include clustering and anomaly detection (Usama et al., 2019).

- Clustering Algorithms: Clustering algorithms, such as k-means and hierarchical clustering, group similar data points together based on their features. In fraud detection, clustering can help identify groups of transactions that deviate significantly from normal behavior, potentially indicating fraudulent activity. However, determining the optimal number of clusters and interpreting the results can be challenging (Gupta, Sharma, & Akhtar, 2021; Qi, Yu, Wang, Liu, & Wang, 2017).
- Anomaly Detection: Anomaly detection algorithms aim to identify outliers or data points that do not conform to the expected pattern. Techniques such as Isolation Forests and Autoencoders are commonly used. Isolation Forests isolate anomalies by randomly partitioning the data. At the same time, Autoencoders, a type of neural network, learn efficient representations of data and flag deviations from the norm as anomalies. These methods are particularly effective for detecting rare and subtle forms of fraud (Gogoi, Bhattacharyya, Borah, & Kalita, 2011).

3.3. Neural Networks

Neural networks, especially deep learning models, have gained prominence in fraud detection due to their ability to model complex and non-linear relationships. These models consist of layers of interconnected nodes (neurons) that process data in a manner inspired by the human brain.

- Feedforward Neural Networks: These are the simplest type of neural network, where data moves in one direction from input to output. They are effective for straightforward classification tasks but may struggle with more complex patterns (Fine, 1999).
- Recurrent Neural Networks (RNNs): RNNs are designed to handle sequential data by maintaining a memory of previous inputs. This makes them suitable for detecting fraud in time-series data, such as transaction histories. However, they can suffer from issues like vanishing gradients, which impede learning in long sequences (Sherstinsky, 2020).
- Convolutional Neural Networks (CNNs): Originally designed for image processing, CNNs have also been applied to fraud detection by transforming transaction data into a format that highlights spatial or hierarchical patterns. Their ability to detect local patterns makes them powerful but computationally intensive (Cheng et al., 2020).

3.4. Applications and Effectiveness

Each machine learning technique is applied to fraud detection in various ways. Supervised learning models are trained on historical transaction data labeled as fraudulent or legitimate. By learning the distinguishing features of fraudulent transactions, these models can predict the likelihood of new fraudulent transactions in real-time. For instance, random forests can handle large volumes of transaction data and provide quick, interpretable results.

On the other hand, unsupervised learning techniques are valuable for discovering new fraud patterns. Clustering can reveal groups of transactions that deviate from normal behavior, prompting further investigation. Anomaly detection algorithms are particularly adept at identifying rare or emerging fraud tactics that supervised models might miss. Neural networks, with their capacity to model complex interactions, are used for more advanced fraud detection scenarios. RNNs can analyze sequences of transactions to detect anomalies over time, while CNNs can identify intricate patterns within transaction data. These models are highly effective but require substantial computational resources and expertise to implement and maintain (Forough & Momtazi, 2021; Okatta, Ajayi, & Olawale, 2024).

3.5. Advantages and Disadvantages

Each machine learning technique has its advantages and disadvantages in the context of fraud detection:

- Supervised Learning: Advantages include high accuracy and interpretability, especially with decision trees and logistic regression. However, these models rely heavily on the availability and quality of labeled data, and they can struggle with detecting new types of fraud not present in the training data.
- Unsupervised Learning: These techniques are excellent for discovering unknown fraud patterns and do not require labeled data. However, they can produce results that are harder to interpret and may require more complex validation methods.

- Neural Networks: Neural networks, particularly deep learning models, can handle complex and high-dimensional data, making them powerful tools for fraud detection. Their main disadvantages include high computational costs, longer training times, and the need for large amounts of data to achieve optimal performance. Additionally, they are often viewed as "black boxes," making their decisions harder to interpret than simpler models.

4. Challenges and Limitations

Implementing machine learning for fraud detection in financial systems presents numerous challenges and limitations. While ML techniques offer significant advantages in identifying fraudulent activities, their application is fraught with complexities that must be addressed to ensure effective and efficient fraud detection.

4.1. Challenges in Implementing Machine Learning for Fraud Detection

One of the primary challenges is data quality. Machine learning models require high-quality, labeled data to train effectively. However, financial data is often messy, incomplete, and imbalanced, with fraudulent transactions significantly outnumbered by legitimate ones. This imbalance can lead to biased models overly sensitive to legitimate transactions, causing high false-positive rates. Moreover, noisy data, which includes errors and irrelevant information, can degrade the performance of ML algorithms, making accurate fraud detection more difficult (Scott, Amajuoyi, & Adeusi, 2024a, 2024b; Udeh, Amajuoyi, Adeusi, & Scott, 2024). Scalability is another significant challenge. Financial institutions process millions of transactions daily, requiring ML models to handle vast amounts of data in real-time. Ensuring that these models can scale efficiently without compromising on performance is crucial. Large-scale data processing demands substantial computational resources and optimized algorithms capable of parallel processing. Additionally, the infrastructure needs to support continuous training and updating of models to adapt to evolving fraud patterns (Wu, Sun, Zhang, Wei, & Chanussot, 2021).

Real-time processing is essential for effective fraud detection, as timely intervention can prevent financial losses and protect customer accounts. However, achieving real-time analysis and decision-making is technically demanding. Machine learning models must process and analyze transactions within milliseconds, which requires advanced stream processing frameworks and low-latency systems. Ensuring real-time capabilities without sacrificing accuracy or significant computational costs is a delicate balance (Santos, Wauters, Volckaert, & De Turck, 2021).

4.2. Limitations of Current Machine Learning Approaches

Despite the advancements in ML, current approaches still have limitations. One of the major limitations is the reliance on historical data. Machine learning models are typically trained on past transaction data, which may not accurately represent future fraud patterns. Fraudsters constantly adapt and develop new techniques, making it challenging for models to predict and identify novel fraud schemes that differ significantly from historical data.

Another limitation is the interpretability of ML models. Many advanced models, particularly deep learning algorithms, are often seen as "black boxes" because their decision-making processes are not easily understood. This lack of transparency can be problematic in a financial context where understanding and explaining decisions is crucial for regulatory compliance and customer trust. Stakeholders, including regulatory bodies, demand clear explanations for why certain transactions are flagged as fraudulent, which is difficult to provide with complex ML models (Buhrmester, Münch, & Arens, 2021).

The issue of false positives also poses a significant limitation. While ML models strive to detect fraudulent transactions accurately, they often flag legitimate transactions as suspicious. High false-positive rates can lead to unnecessary customer friction, loss of trust, and operational inefficiencies as more resources are required to review and verify flagged transactions manually. Balancing the trade-off between minimizing false positives and maximizing fraud detection accuracy remains a challenging aspect of ML deployment in financial fraud detection.

4.3. Ethical and Privacy Concerns

Using machine learning in financial transactions raises several ethical and privacy concerns that must be addressed to ensure responsible and fair deployment. One of the primary ethical concerns is bias in ML models. If the training data contains biases, the resulting models may perpetuate these biases, leading to unfair treatment of certain groups of customers. For example, suppose a model is trained on data that overrepresents a particular demographic as being more prone to fraud. In that case, it may unfairly target transactions from individuals within that demographic, resulting in discriminatory practices. Privacy concerns are paramount in the context of financial data. Machine learning models

require access to vast amounts of sensitive financial information to function effectively. Ensuring this data is collected, stored, and processed in compliance with data protection regulations such as the General Data Protection Regulation (GDPR) is critical. Financial institutions must implement robust data anonymization and encryption techniques to protect customer privacy and prevent unauthorized access to sensitive information (Shukla, George, Tiwari, & Kureethara, 2022).

Moreover, the transparency of ML models is linked to ethical considerations. Customers and regulatory bodies have the right to understand how their data is being used and how decisions regarding their transactions are made. The opaque nature of many ML models can hinder transparency and accountability, making it difficult to ensure that decisions are fair and justifiable. Developing methods for improving the interpretability and explainability of ML models is essential for addressing these concerns. Finally, the potential misuse of machine learning poses ethical risks. There is a risk that ML models designed for fraud detection could be repurposed for other, less ethical uses, such as surveillance or profiling. Establishing clear guidelines and regulations for using ML in financial systems can help mitigate these risks and ensure the technology is used responsibly (Diaz et al., 2021; Fritz-Morgenthal, Hein, & Papenbrock, 2022).

5. Future Directions and Conclusion

The future of financial fraud prevention using machine learning is poised to witness significant advancements and emerging trends that promise to enhance the effectiveness and efficiency of fraud detection systems. As financial fraud schemes become increasingly sophisticated, applying advanced ML techniques and interdisciplinary approaches will be critical in staying ahead of fraudsters.

5.1. Emerging Trends and Advancements

Integrating artificial intelligence with blockchain technology is one of the most promising emerging trends. Blockchain's inherent transparency and immutability make it an excellent secure transaction recording and verification tool. When combined with AI and ML, blockchain can enhance fraud detection capabilities by providing a reliable transaction data source, reducing the risk of data tampering. Smart contracts, self-executing contracts with the terms directly written into code, can also be used to automate and enforce rules in real-time, further reducing the opportunity for fraud.

Another significant trend is the adoption of federated learning. This approach allows machine learning models to be trained across multiple decentralized devices or servers holding local data samples without exchanging them. Federated learning enhances privacy and security by ensuring that sensitive financial data does not leave its source, addressing one of the primary ethical concerns in ML-based fraud detection. This method also allows for developing more robust models by leveraging diverse datasets from different institutions.

The use of explainable AI (XAI) is gaining traction as well. XAI aims to make the decision-making processes of ML models more transparent and understandable to humans. This is particularly important in financial fraud detection, where understanding the rationale behind a model's prediction is crucial for regulatory compliance and maintaining customer trust. Techniques such as LIME (Local Interpretable Model-agnostic Explanations) and SHAP (SHapley Additive exPlanations) are being developed to provide clear insights into how models arrive at their decisions.

5.2. Potential Improvements and Future Research Areas

Several areas offer potential for further research and improvement in ML-based fraud detection. One key area is the enhancement of data quality and preprocessing techniques. Developing methods to better handle noisy, incomplete, and imbalanced data will significantly improve model accuracy and reliability. Techniques such as synthetic data generation and advanced anomaly detection algorithms can be explored to address these issues.

Another area of focus is the continuous learning and adaptation of ML models. Fraudsters constantly evolve their tactics, necessitating models that can quickly adapt to new patterns of fraudulent behavior. Research into online learning and reinforcement learning can contribute to developing models that learn and update continuously, ensuring they remain effective over time. Interdisciplinary collaboration between finance, cybersecurity, and data science experts is also essential for advancing fraud detection technologies. Combining knowledge from these fields can lead to more comprehensive and innovative solutions. Additionally, establishing industry standards and best practices for the ethical use of ML in fraud detection will be crucial for fostering trust and ensuring responsible deployment.

Machine learning has significantly impacted the field of financial fraud detection, offering advanced tools and techniques to enhance transaction security and prevent fraudulent activities. While there are challenges and limitations to overcome, the potential benefits of ML are immense. Financial institutions can develop more effective and trustworthy

fraud detection systems by continuously advancing ML technologies, improving data quality, and addressing ethical concerns. The future of fraud prevention lies in integrating cutting-edge technologies, interdisciplinary collaboration, and a commitment to ethical practices. As these elements come together, the financial industry will be better equipped to protect itself against the ever-evolving threat of fraud, ensuring the security and integrity of financial transactions for all stakeholders involved.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Albshaier, L., Almarri, S., & Hafizur Rahman, M. (2024). A review of blockchain's role in E-Commerce transactions: Open challenges, and future research directions. Computers, 13(1), 27.

[2] Antoniadi, A. M., Du, Y., Guendouz, Y., Wei, L., Mazo, C., Becker, B. A., & Mooney, C. (2021). Current challenges and future opportunities for XAI in machine learning-based clinical decision support systems: a systematic review. Applied Sciences, 11(11), 5088.

[3] Bangdiwala, S. I. (2018). Regression: binary logistic. International journal of injury control and safety promotion, 25(3), 336-338.

[4] Bhargava, N., Sharma, G., Bhargava, R., & Mathuria, M. (2013). Decision tree analysis on j48 algorithm for data mining. Proceedings of international journal of advanced research in computer science and software engineering, 3(6).

[5] Bhatia, N. L., Shukla, V. K., Punhani, R., & Dubey, S. K. (2021). Growing aspects of cyber security in e-commerce. Paper presented at the 2021 International Conference on Communication information and Computing Technology (ICCICT).

[6] Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. Statistical science, 17(3), 235-255.

[7] Buhrmester, V., Münch, D., & Arens, M. (2021). Analysis of explainers of black box deep neural networks for computer vision: A survey. Machine Learning and Knowledge Extraction, 3(4), 966-989.

[8] Carcillo, F., Le Borgne, Y.-A., Caelen, O., Kessaci, Y., Oblé, F., & Bontempi, G. (2021). Combining unsupervised and supervised learning in credit card fraud detection. Information sciences, 557, 317-331.

[9] Cheng, D., Xiang, S., Shang, C., Zhang, Y., Yang, F., & Zhang, L. (2020). Spatio-temporal attention-based neural network for credit card fraud detection. Paper presented at the Proceedings of the AAAI conference on artificial intelligence.

[10] Diaz, O., Kushibar, K., Osuala, R., Linardos, A., Garrucho, L., Igual, L., . . . Lekadir, K. (2021). Data preparation for artificial intelligence in medical imaging: A comprehensive guide to open-access platforms and tools. Physica medica, 83, 25-37.

[11] Fine, T. L. (1999). Feedforward neural network methodology: Springer Science & Business Media.

[12] Forough, J., & Momtazi, S. (2021). Ensemble of deep sequential models for credit card fraud detection. Applied Soft Computing, 99, 106883.

[13] Fritz-Morgenthal, S., Hein, B., & Papenbrock, J. (2022). Financial risk management and explainable, trustworthy, responsible AI. Frontiers in artificial intelligence, 5, 779799.

[14] Gogoi, P., Bhattacharyya, D. K., Borah, B., & Kalita, J. K. (2011). A survey of outlier detection methods in network anomaly identification. The Computer Journal, 54(4), 570-588.

[15] Gupta, A., Sharma, H., & Akhtar, A. (2021). A comparative analysis of k-means and hierarchical clustering. EPRA International Journal of Multidisciplinary Research (IJMR), 7(8).

[16] 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.

[17] Hussain, S. F. (2019). A novel robust kernel for classifying high-dimensional data using Support Vector Machines. Expert systems With applications, 131, 116-131.

[18] Ilori, O., Nwosu, N. T., & Naiho, H. N. N. (2024). A comprehensive review of it governance: effective implementation of COBIT and ITIL frameworks in financial institutions. Computer Science & IT Research Journal, 5(6), 1391-1407.

[19] Kaur, S., Kaur, G., & Shabaz, M. (2022). A Secure Two-Factor Authentication Framework in Cloud Computing. Security and Communication Networks, 2022(1), 7540891.

[20] Mahtani, U. (2022). Fraudulent practices and blockchain accounting systems. Journal of Accounting, Ethics and Public Policy, 23(1), 97-148.

[21] Nakitende, M. G., Rafay, A., & Waseem, M. (2024). Frauds in business organizations: A comprehensive overview. Research Anthology on Business Law, Policy, and Social Responsibility, 848-865.

[22] Nicholls, J., Kuppa, A., & Le-Khac, N.-A. (2021). Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. IEEE Access, 9, 163965-163986.

[23] Niu, X., Wang, L., & Yang, X. (2019). A comparison study of credit card fraud detection: Supervised versus unsupervised. arXiv preprint arXiv:1904.10604.

[24] Nwaimo, C. S., Adegbola, A. E., & Adegbola, M. D. (2024). Predictive analytics for financial inclusion: Using machine learning to improve credit access for under banked populations. Computer Science & IT Research Journal, 5(6), 1358-1373.

[25] Nwaimo, C. S., Adegbola, A. E., Adegbola, M. D., & Adeusi, K. B. (2024). Forecasting HR expenses: A review of predictive analytics in financial planning for HR. International Journal of Management & Entrepreneurship Research, 6(6), 1842-1853.

[26] Nwobodo, L. K., Nwaimo, C. S., & Adegbola, M. D. (2024). Strategic financial decision-making in sustainable energy investments: Leveraging big data for maximum impact. International Journal of Management & Entrepreneurship Research, 6(6), 1982-1996.

[27] Nwosu, N. T., & Ilori, O. (2024). Behavioral finance and financial inclusion: A conceptual review and framework development.

[28] Okatta, C. G., Ajayi, F. A., & Olawale, O. (2024). Navigating the future: integrating AI and machine learning in hr practices for a digital workforce. Computer Science & IT Research Journal, 5(4), 1008-1030.

[29] Oriji, O., Shonibare, M. A., Daraojimba, R. E., Abitoye, O., & Daraojimba, C. (2023). Financial technology evolution in Africa: a comprehensive review of legal frameworks and implications for ai-driven financial services. International Journal of Management & Entrepreneurship Research, 5(12), 929-951.

[30] Pomerleau, P.-L., & Lowery, D. L. (2020). Countering Cyber Threats to Financial Institutions. In A Private and Public Partnership Approach to Critical Infrastructure Protection: Springer.

[31] Qi, J., Yu, Y., Wang, L., Liu, J., & Wang, Y. (2017). An effective and efficient hierarchical K-means clustering algorithm. International Journal of Distributed Sensor Networks, 13(8), 1550147717728627.

[32] Santos, J., Wauters, T., Volckaert, B., & De Turck, F. (2021). Towards low-latency service delivery in a continuum of virtual resources: State-of-the-art and research directions. IEEE Communications Surveys & Tutorials, 23(4), 2557-2589.

[33] Sarker, I. H. (2021). Deep learning: a comprehensive overview on techniques, taxonomy, applications and research directions. SN computer science, 2(6), 420.

[34] Scheaf, D. J., & Wood, M. S. (2022). Entrepreneurial fraud: A multidisciplinary review and synthesized framework. Entrepreneurship Theory and Practice, 46(3), 607-642.

[35] Scott, A. O., Amajuoyi, P., & Adeusi, K. B. (2024a). Effective credit risk mitigation strategies: Solutions for reducing exposure in financial institutions. Magna Scientia Advanced Research and Reviews, 11(1), 198-211.

[36] Scott, A. O., Amajuoyi, P., & Adeusi, K. B. (2024b). Theoretical perspectives on risk management strategies in financial markets: Comparative review of African and US approaches. International Journal of Management & Entrepreneurship Research, 6(6), 1804-1812.

[37] Sherstinsky, A. (2020). Fundamentals of recurrent neural network (RNN) and long short-term memory (LSTM) network. Physica D: Nonlinear Phenomena, 404, 132306.

[38] Shukla, S., George, J. P., Tiwari, K., & Kureethara, J. V. (2022). Data security. In Data Ethics and Challenges (pp. 41-59): Springer.

[39] Trivedi, N. K., Simaiya, S., Lilhore, U. K., & Sharma, S. K. (2020). An efficient credit card fraud detection model based on machine learning methods. International Journal of Advanced Science and Technology, 29(5), 3414-3424.

[40] Udeh, E. O., Amajuoyi, P., Adeusi, K. B., & Scott, A. O. (2024). The role of big data in detecting and preventing financial fraud in digital transactions.

[41] Usama, M., Qadir, J., Raza, A., Arif, H., Yau, K.-L. A., Elkhatib, Y., . . . Al-Fuqaha, A. (2019). Unsupervised machine learning for networking: Techniques, applications and research challenges. IEEE Access, 7, 65579-65615.

[42] Usmani, U. A., Happonen, A., & Watada, J. (2022). A review of unsupervised machine learning frameworks for anomaly detection in industrial applications. Paper presented at the Science and Information Conference.

[43] Villányi, B. (2021). Money laundering: History, regulations, and techniques. In Oxford Research Encyclopedia of Criminology and Criminal Justice.

[44] Wu, Z., Sun, J., Zhang, Y., Wei, Z., & Chanussot, J. (2021). Recent developments in parallel and distributed computing for remotely sensed big data processing. Proceedings of the IEEE, 109(8), 1282-1305.

[45] Xu, Y., Zhou, Y., Sekula, P., & Ding, L. (2021). Machine learning in construction: From shallow to deep learning. Developments in the built environment, 6, 100045.