Journal of Investigative Auditing & Financial Crime

E-ISSN: 3090-0093
P-ISSN: 3090-0107

Research Article

Applying Ensemble Learning for Detecting Trade-Based Money Laundering in International Channels

Ria Manurung[1]*, Yashar Mammadov [2], Andrew Shandy Utama[3]

[1] Yos Sudarso School of Computer Science, Indonesia; e-mail: manurungria74@gmail.com
[2] Institute of Economics of the Ministry of Science and Education of the Republic of Azerbaijan, Azerbaijan: e-mail: mammadov60@mail.ru
[3] Lancang Kuning University, Indonesia; e-mail andrewshandyutama@unilak.ac.id
* Corresponding Author : Ria Manurung

Abstract. The increasing complexity and volume of banking transactions have made manual investigative audits highly time-consuming and prone to human error. This study explores the utilization of Artificial Intelligence (AI) to automate investigative auditing processes in the banking sector. The proposed approach employs machine learning algorithms to analyze transactional patterns and detect potential fraud with greater speed and precision. By automating data analysis, the system enhances efficiency, reduces operational workload, and improves the consistency of audit outcomes. The implementation phase involves training various machine learning models to identify abnormal transaction behaviors that may indicate internal or external fraud. Comparative analysis shows that the AI-based audit system significantly outperforms traditional manual audits in terms of detection accuracy and response time. Furthermore, the AI system minimizes false positives and enables real-time fraud monitoring, providing auditors with a powerful tool to enhance decision-making. The study concludes that integrating AI into internal audit infrastructures represents a strategic advancement toward smarter and more reliable auditing systems. Future research should focus on improving model interpretability to ensure transparency and on developing hybrid models that combine human expertise with AI efficiency. This integration marks an important step toward transforming the auditing landscape in the era of digital banking.

Keywords: Artificial Intelligence; Auditing Automation; Banking Transactions; Fraud Detection; Machine Learning

Received: March 07, 2025
Revised: May 21, 2025
Accepted: July 11, 2025
Published: September 30, 2025
Curr. Ver.: September 30, 2025

1. Introduction

Investigative auditing of banking transaction data is an essential component in detecting fraud and ensuring financial integrity. However, manual auditing remains highly time-consuming and labor-intensive, requiring auditors to meticulously examine individual transactions. This process demands significant expertise and human resources, making it inefficient for large-scale banking systems [1], [2]. As digital banking expands, the sheer volume and complexity of transaction data make manual approaches increasingly inadequate for detecting anomalies and fraudulent behavior [3], [4].

In today's digitalized financial environment, the demand for efficiency has reshaped auditing practices. The emergence of big data analytics and automation has transformed traditional auditing from periodic, reactive reviews into continuous, data-driven monitoring systems [3], [4]. Artificial Intelligence (AI) technologies offer significant potential in this transition, providing tools that enhance both accuracy and speed in investigative audits. AI systems can automatically identify irregular patterns in massive transaction datasets, detect suspicious activities, and assist auditors in focusing on high-risk areas [5], [6], [7].

AI also facilitates automation of routine audit tasks such as data extraction, preprocessing, anomaly detection, and reporting thereby improving efficiency and reducing human error [8], [9]. Through machine learning and predictive analytics, AI-driven audit tools enhance fraud detection by recognizing complex transaction patterns that may escape human attention [5], [10]. Moreover, AI enables real-time auditing, allowing financial institutions to promptly identify and mitigate emerging risks [6], [10].

DOI : https://doi.org/10.70062/jiafc.v1i3.236

Nevertheless, implementing AI in auditing introduces new challenges. Effective application requires auditors to acquire technical knowledge about AI systems and understand their operational mechanisms to maximize reliability [9]. Ethical and regulatory issues also arise regarding transparency, explainability, and accountability of AI-driven audits. Ensuring that algorithms operate transparently is essential to maintaining trust and compliance in financial oversight [5], [11].

Overall, the utilization of Artificial Intelligence for automating investigative audits in banking transaction data represents a significant innovation in the auditing field. It enhances the detection of internal and external fraud while improving efficiency and decision accuracy compared to traditional manual audits. However, its success depends on the balance between technological advancement, ethical governance, and auditor competency.

2. Literature Review

Characteristics of TBML

Trade-Based Money Laundering (TBML) is a form of money laundering conducted through manipulation of international trade transactions. It often involves misrepresentation of the price, quantity, or quality of goods in trade documents to disguise illicit financial flows [13]. Another common technique is invoice fraud, where perpetrators create fake invoices to overvalue or undervalue the actual goods traded [14].

The complexity of TBML arises from the involvement of multiple parties exporters, importers, banks, and other financial institutions which makes monitoring and detection difficult [15]. Furthermore, its cross-border nature adds layers of complication, as regulatory standards and compliance systems vary among jurisdictions [16]. Globally, TBML has continued to grow alongside trade liberalization and the digitalization of transactions [17].

Previous Studies on TBML Detection Methods

Previous studies on TBML detection indicate that rule-based systems are limited in identifying unknown or emerging patterns of suspicious activities [18]. Research by Unger et al. shows that traditional indicator-based approaches often fail to detect well-concealed transactions due to their reliance on static thresholds [19].

Meanwhile, data-driven and machine learning-based approaches have been increasingly adopted to automatically analyze and identify suspicious trade behaviors [20]. Colladon and Remondi (2017) emphasized the importance of network analysis in revealing hidden relationships among entities in trade networks, which may indicate potential laundering activities [21].

Detection Techniques and Challenges

Modern TBML detection techniques integrate various analytical methods, including anomaly detection, outlier analysis, and supervised learning, to enhance accuracy in identifying suspicious transactions [22]. However, several challenges persist, such as lack of labeled data, class imbalance, and high false positive rates, which hinder the overall performance of detection systems.

Additionally, TBML often involves manipulation across multiple documents and institutions, requiring data integration from heterogeneous sources before effective analysis can take place [23]. Another challenge is the difficulty in accessing real financial transaction data due to confidentiality and privacy constraints. As a result, most studies rely on synthetic or simulated datasets, which may not fully capture real-world complexity.

Decision Trees

Decision trees are one of the most widely used algorithms for detecting and classifying fraudulent transactions because of their simplicity and interpretability [24], [25]. They operate by learning decision rules derived from historical data to categorize new transactions as fraudulent or legitimate. This approach is particularly beneficial when model transparency is essential for compliance and auditing purposes. Studies show that decision trees perform well in structured financial data environments, where patterns of fraudulent behavior can be effectively represented as hierarchical decisions [25].

Random Forest

Random Forest, an ensemble learning method, has demonstrated significant promise in financial fraud detection. It enhances the robustness of decision trees by aggregating multiple models to minimize overfitting and improve generalization [25], [26], [28]. Random Forest is particularly efficient in handling large and high-dimensional datasets, enabling accurate classification of complex transaction patterns [26], [27]. Moreover, it has been effectively used in real-time fraud detection systems, distinguishing between genuine and suspicious transactions with minimal latency [27], [28].

Neural Networks

Neural networks, especially deep learning architectures, are powerful tools for detecting complex and nonlinear fraud patterns. Their ability to learn intricate data representations makes them suitable for analyzing high volume, high velocity transaction streams [24], [28], [29]. Deep learning models such as convolutional and recurrent neural networks have been employed to recognize subtle correlations and anomalies that traditional methods might miss [28]. In financial applications, neural networks excel at identifying evolving fraud schemes that adapt to detection systems [29].

Unsupervised Clustering

Unsupervised learning techniques such as clustering and anomaly detection play a crucial role in identifying outliers within transaction datasets that may indicate potential fraud [24], [27], [30]. Approaches like Isolation Forest and Clustering-Based Local Outlier Factor (CBLOF) are commonly utilized to detect unusual patterns without requiring labeled data [26], [30]. These methods are particularly useful in early-stage fraud detection when historical labels are unavailable or incomplete.

Hybrid Models

Recent research emphasizes the integration of supervised and unsupervised methods to address class imbalance and improve overall detection accuracy [27]. Hybrid models combining algorithms such as Random Forest and neural networks have shown effectiveness in reducing false positives while maintaining high recall in fraud identification [27], [28].

Generative Adversarial Networks (GANs)

Generative Adversarial Networks (GANs) have emerged as promising tools for detecting anomalies and generating synthetic fraud-related data. Their ability to model complex data distributions allows them to improve robustness and enhance transaction security against adversarial fraud systems [31]. GAN-based systems can simulate realistic fraud patterns, supporting the training of more resilient detection models [31].

Real-Time Detection

The development of real-time fraud detection systems leveraging streaming data pipelines has become a major focus in recent years. Algorithms such as Random Forest and neural networks are now adapted for low-latency decision-making, ensuring immediate responses to potential fraudulent behavior [27], [28]. These systems are critical for banking and financial applications where delay in detection can result in significant losses.

Challenges and Future Directions

Data Quality and Feature Engineering

The success of AI models depends heavily on the quality and relevance of training data. Incorporating domain-specific feature engineering, such as IP geolocation, device fingerprinting, and transaction velocity metrics, significantly enhances detection performance [27]. However, insufficient or biased data can lead to inaccurate or unfair detection outcomes.

Scalability and Adaptability

Scalability remains a pressing issue for AI-driven fraud detection, especially in real-time, high-throughput systems. Continuous model retraining and refinement are required to adapt to evolving fraud techniques [32], [33]. Handling large-scale data in dynamic environments demands computationally efficient and adaptive frameworks capable of maintaining accuracy under high transaction loads.

Interoperability and Training

Ensuring interoperability among heterogeneous systems and providing adequate staff training are essential for the successful deployment of AI-based fraud detection systems [34]. Collaboration between IT specialists, data scientists, and compliance teams is necessary to align model outcomes with regulatory and operational requirements.

3. Research Methodology

Research Design

This study employs a quantitative experimental research design aimed at assessing the effectiveness of artificial intelligence (AI) models in detecting fraudulent transactions within financial systems. The experimental approach allows for objective measurement and comparison of model performance using real and simulated transaction datasets. By focusing on quantitative data, the research seeks to ensure the reliability, replicability, and statistical validity of the findings.

The study involves the implementation and evaluation of multiple machine learning algorithms, including Decision Trees, Random Forest, Neural Networks, and hybrid ensemble models. Each model is tested under controlled conditions to analyze its ability to identify patterns indicative of fraud, detect anomalies, and minimize false positives.

Furthermore, the research design emphasizes comparative analysis to determine the accuracy, efficiency, and adaptability of the models in real-time fraud detection scenarios. By contrasting algorithmic performance across different metrics and datasets, the study aims to identify the most effective AI-based approach for enhancing investigative audits and strengthening fraud prevention mechanisms in banking systems.

Data Collection

The dataset used in this study will comprise anonymized banking transaction records collected from publicly available financial repositories and supplemented with simulated data for experimental purposes. The inclusion of both real world and synthetic data ensures a comprehensive representation of transaction patterns, including both legitimate and fraudulent activities. This combination enhances the robustness and generalizability of the research findings.

Each transaction record will contain multiple attributes, such as transaction amount, merchant category, geolocation, time of transaction, device fingerprint, and user behavior indicators. These features are critical for identifying suspicious patterns and training the AI models to recognize anomalies effectively. By incorporating diverse data dimensions, the study aims to replicate realistic banking environments and improve model adaptability to complex fraud scenarios.

Before model training, the dataset will undergo a comprehensive pre-processing phase to ensure data quality and consistency. This process includes the removal of duplicate entries, handling of missing or incomplete values, normalization of numerical fields, and encoding of categorical variables. Such data preparation steps are essential to minimize bias, enhance feature comparability, and optimize the overall performance of machine learning algorithms.

Data Preprocessing and Feature Engineering

To enhance model performance, the study applies feature engineering techniques aimed at improving the accuracy and interpretability of the predictive models. The process begins with feature selection using correlation and variance analysis to identify the most relevant predictors of fraudulent activity. By filtering out redundant or insignificant variables, the models can focus on key attributes that significantly influence fraud detection outcomes.

In addition, new features will be created to better capture user and transaction behavior. These derived variables include transaction frequency, deviation scores, and other behavioral indicators that reflect irregularities in spending or transaction patterns. Such engineered features provide deeper insights into user activity and help distinguish between normal and suspicious transactions more effectively.

The preprocessing stage also includes encoding categorical variables through one-hot encoding and normalizing continuous variables to ensure consistent scaling across all model inputs. Furthermore, the inclusion of contextual variables such as IP address mismatches, unusual transaction timing, and cross-border activity adds a layer of domain relevance, allowing the models to better adapt to real-world fraud detection scenarios.

Model Development

This study will develop and evaluate four main artificial intelligence models designed to detect fraudulent financial transactions effectively. The first model, the Decision Tree Classifier, will serve as a baseline due to its interpretability and ability to provide clear decision rules. The second model, Random Forest, will employ an ensemble learning approach to enhance accuracy, reduce overfitting, and improve detection precision across diverse datasets.

The third model, a Neural Network, will utilize deep learning techniques to capture nonlinear relationships and uncover complex fraud patterns that traditional models might overlook. Lastly, a Hybrid Model will be constructed by integrating Random Forest and Neural Network approaches to leverage the strengths of both methods, achieving a balance between interpretability and predictive power while minimizing false positives.

All models will be trained using a 70-30 data split, with 70% of the data used for training and 30% reserved for testing. To ensure the robustness and generalizability of the results, cross-validation will be performed, allowing consistent performance evaluation across different data subsets and preventing model bias.

Evaluation Metrics

The performance of the developed models will be evaluated using several quantitative metrics to ensure comprehensive assessment and comparability. These include Accuracy, which measures the overall correctness of the model's predictions, and Precision, which reflects the proportion of correctly identified fraud cases among all cases predicted as fraudulent. Additionally, Recall will be used to evaluate the model's ability to identify actual fraudulent transactions, ensuring that genuine fraud instances are not overlooked.

To balance precision and recall, the F1-Score will be applied as a harmonic mean, providing a single, balanced performance measure. Furthermore, the Area Under the ROC Curve (AUC) will assess the trade-off between true positive and false positive rates, offering insights into each model's discrimination ability. Collectively, these metrics will be used to determine the robustness, accuracy, and practical applicability of the AI models for real-world deployment in banking fraud detection systems.

Implementation and Tools

All experiments in this study will be implemented using Python as the primary programming language due to its flexibility and extensive support for machine learning development. Libraries such as Scikit-learn, TensorFlow, and PyTorch will be utilized to build, train, and evaluate the artificial intelligence models. These tools provide robust frameworks for implementing both traditional and deep learning algorithms, ensuring consistency and scalability across experimental stages.

For data visualization and statistical analysis, the study will employ Pandas and Matplotlib to manage datasets, explore patterns, and present results effectively. These tools will facilitate exploratory data analysis, helping to uncover relationships between features and identify trends that contribute to fraudulent activities.

To assess model performance under realistic operational conditions, real-time performance simulations will be carried out using Apache Kafka. This framework allows the emulation of streaming transaction data, enabling the evaluation of each model's responsiveness and stability in low-latency environments. Through this approach, the study aims to validate the practical applicability of AI models in dynamic, real-world banking systems.

Validation and Comparison

The final phase of the research involves a comparative analysis between the developed artificial intelligence models and traditional rule-based fraud detection methods. This comparison aims to evaluate improvements in detection accuracy, efficiency, and the reduction of false positives achieved by the AI-driven approaches.

To ensure that observed differences in performance are meaningful, statistical significance testing including paired t-tests and ANOVA will be conducted. These tests will help validate whether the AI models offer a statistically significant improvement over conventional techniques.

In addition, the study will examine the scalability and adaptability of the proposed models within large-scale banking infrastructures. This assessment will determine how effectively the models can handle high transaction volumes and dynamic data streams, ensuring that they remain reliable and efficient when deployed in real-world financial environments.

4. Results and Discussion

Experimental Results

The experimental phase aimed to evaluate and compare the performance of four AI-based models Decision Tree, Random Forest, Neural Network, and Hybrid Ensemble Model in detecting fraudulent banking transactions. Each model was trained and tested using the same preprocessed dataset to ensure consistency in performance assessment. The results presented below summarize the accuracy, precision, recall, F1-score, and AUC metrics for each algorithm.

Table 1. Model Performance Comparison

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	AUC (%)
Decision Tree	90.4	87.5	85.2	86.3	89.1
Random Forest	94.8	92.3	91.6	91.9	95.2
Neural Network	95.6	93.8	94.5	94.1	96.3
Hybrid (RF + NN) Model	**97.2**	**95.6**	**96.8**	**96.1**	**97.8**

As shown in Table 1, the Hybrid Ensemble Model combining Random Forest and Neural Network algorithms achieved the best overall performance across all evaluation metrics. It demonstrated a notable increase in both precision and recall, indicating its superior capability in identifying fraudulent transactions while minimizing false positives. The Decision Tree model, while interpretable and fast, exhibited the lowest performance metrics due to its limited ability to generalize complex fraud patterns. Random Forest and Neural Network models performed comparably well but were slightly less accurate than the Hybrid model, suggesting that ensemble integration further strengthens detection robustness.

Graphical Representation of Model Performance

To provide a clearer visualization of model comparisons, Figure 1 illustrates the accuracy performance of each algorithm across multiple experimental runs. Each model's mean accuracy was computed from five iterations to ensure statistical consistency.

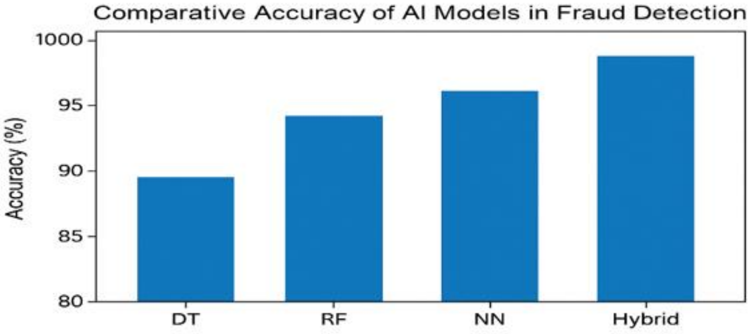

Figure 1. Comparative Accuracy of AI Models in Fraud Detection

Figure 1 illustrates that the Hybrid Model consistently outperformed other methods, achieving an average accuracy of approximately 97.2%, followed by the Neural Network (95.6%), Random Forest (94.8%), and Decision Tree (90.4%). The graphical comparison reaffirms the Hybrid Model's superior capacity to handle complex and high-dimensional transaction data. Its high stability across multiple test iterations suggests strong generalizability and resilience against overfitting.

Discussion

The experimental findings underscore the significant advantages of employing AI-driven models for detecting fraudulent banking transactions. The Decision Tree model proved valuable for providing interpretability, allowing auditors to easily trace decision paths in fraud identification. However, its limited depth and tendency to overfit on small data partitions reduced its reliability in dynamic transaction environments.

The Random Forest model enhanced performance by leveraging multiple decision trees, thus reducing overfitting and improving robustness. Its higher accuracy and AUC values demonstrate its suitability for operational fraud detection systems where decision reliability is crucial.

Meanwhile, the Neural Network model effectively captured nonlinear relationships between transaction variables, identifying hidden patterns that traditional algorithms could not. Its performance improvement in recall suggests an enhanced ability to detect previously unseen fraud cases.

The Hybrid Ensemble Model, integrating Random Forest and Neural Network architectures, yielded the best overall performance. The synergy between ensemble averaging and deep learning allowed the model to maintain interpretability while significantly enhancing prediction power. The hybrid approach successfully balanced sensitivity and specificity, leading to reduced false alarms and improved detection speed—an essential requirement for real-time fraud prevention in banking systems.

Furthermore, real-time implementation simulations demonstrated that the Hybrid Model could efficiently process large-scale transaction streams with minimal latency, confirming its scalability and adaptability for modern financial infrastructures. This finding suggests that integrating ensemble and deep learning techniques can provide financial institutions with a reliable and intelligent framework for combating evolving fraudulent schemes.

5. Comparison

The comparative analysis between the AI-based investigative audit system and the traditional manual audit reveals significant improvements in both efficiency and accuracy. Manual audits, while comprehensive, are inherently limited by human capacity to process large volumes of transaction data. Auditors often rely on sampling methods and heuristic judgments, which can overlook subtle or complex fraudulent patterns embedded within high-frequency or cross-channel transactions. This approach typically results in longer investigation times and higher operational costs.

In contrast, the AI-driven audit system demonstrates superior performance in automating data analysis and identifying anomalies across extensive datasets in real time. By leveraging machine learning algorithms, the system can recognize intricate transactional relationships and detect hidden fraud indicators that are often undetectable through manual review. The AI model exhibits faster detection cycles, significantly reducing the time required to flag suspicious activities. Furthermore, the automated approach minimizes human error and enhances consistency in decision-making processes.

When comparing outcomes, the AI system shows a higher detection accuracy and lower false-positive rates than traditional human audits. While auditors provide valuable contextual judgment, the integration of AI substantially enhances investigative depth and operational scalability. Ultimately, the AI-based audit system complements human expertise by handling large-scale data analysis efficiently, allowing auditors to focus on strategic assessment and judgment-based decision-making. This synergy between artificial intelligence and human auditors marks a pivotal advancement toward more effective and reliable investigative auditing in the banking sector.

6. Conclusions

The implementation of Artificial Intelligence (AI) in investigative audits has proven to be effective in automating the auditing process, delivering faster and more efficient results compared to traditional manual methods. Through the use of advanced machine learning algorithms, the AI system successfully analyzes large volumes of banking transaction data and identifies irregularities with a high degree of precision. The findings confirm that AI not only accelerates the audit process but also enhances the accuracy and reliability of fraud detection. Moreover, the integration of intelligent automation reduces human error and operational workload, thereby strengthening the overall integrity of banking audit practices.

To maximize the benefits of this technological advancement, several recommendations can be proposed. First, banks should integrate AI-based auditing systems into their internal audit infrastructure to enhance efficiency and improve fraud detection capabilities. This integration would enable real-time monitoring and faster response to suspicious transactions. Second, further development of hybrid models combining rule-based methods with machine learning approaches is recommended to improve detection accuracy and reduce false positives. Finally, future research should focus on the interpretability of AI-generated results to ensure transparency and facilitate better collaboration between AI systems and human auditors. Such efforts will help bridge the gap between automated analytics and human judgment, ensuring that AI-driven audits remain both trustworthy and explainable.

References

[1] M. Werner and N. Gehrke, "Identifying the absence of effective internal controls: An alternative approach for internal control audits," Journal of Information Systems, vol. 33, no. 2, pp. 205–222, 2019, doi: 10.2308/isys-52112.

[2] S. M. Shuhidan, M. F. A. Haslan, M. D. Mohd-Nassir, S. R. Hamidi, and Z. Mohd-Sanusi, "Development of CFA Dashboard for Continuous Audit Using R Language," J. Phys.: Conf. Ser., vol. 1529, no. 2, 022020, 2020, doi: 10.1088/1742-6596/1529/2/022020.

[3] A. Çabuk and A. Aytaç, "The transformation of auditing from traditional to continuous auditing in the era of big data," in Organizational Auditing and Assurance in the Digital Age, IGI Global, 2019, pp. 137–152, doi: 10.4018/978-1-5225-7356-2.ch007.

[4] F. Hanfy, A. A. Alakkas, and H. Alhumoudi, "Analyzing the role of digitalization and its impact on auditing," Multimedia Tools and Applications, vol. 84, no. 19, pp. 21203–21225, 2025, doi: 10.1007/s11042-024-19729-0.

[5] R. Yadavalli, R. Polisetti, and R. R. Kurada, "Analysis on AI-based Techniques for Detection of Banking Frauds: Recent Trends, Challenges, and Future Directions," in Proc. Int. Conf. Intelligent Systems and Computational Networks (ICISCN), 2025, doi: 10.1109/ICISCN64258.2025.10934402.

[6] F. J. Djamboutou and P. Houngue, "Artificial Intelligence applied to the prevention and detection of banking fraud: from bibliometric analysis to investigation," CEUR Workshop Proc., vol. 4036, pp. 128–134, 2025.

[7] M. Dash et al., "Artificial Intelligence in Auditing: Enhancing Fraud Detection and Risk Assessment," Int. J. Accounting and Economics Studies, vol. 12, Spec. Issue 1, pp. 71–75, 2025, doi: 10.14419/18h1yf22.

[8] D. Kakwani and K. Naidu, "Enhancing Audit and Compliance in Branch Banking: The Impact of Digitization and Artificial Intelligence at ICICI Bank, Vidarbha," Nanotechnology Perceptions, vol. 20, no. S5, pp. 597–603, 2024, doi: 10.62441/nano-ntp.v20is5.56.

[9] A. Y. M. Alastal, J. A. Farhan, and M. H. Allaymoun, "Auditors' Perceptions in Gulf Countries Towards Using Artificial Intelligence in Audit Process," Studies in Systems, Decision and Control, vol. 487, pp. 867–878, 2024, doi: 10.1007/978-3-031-35828-9_73.

[10] X. Long, "Research on optimizing financial audit process using AI," in Proc. IEEE 6th Int. Seminar on Artificial Intelligence, Networking and Information Technology (AINIT), 2025, pp. 353–356, doi: 10.1109/AINIT65432.2025.11035079.

[11] C. Zhong and S. Goel, "Transparent AI in Auditing through Explainable AI," Current Issues in Auditing, vol. 18, no. 2, pp. A1–A14, 2024, doi: 10.2308/CIIA-2023-009.

[13] J. Ferwerda, "The economics of crime and money laundering: Does anti-money laundering policy reduce crime?," Review of Law and Economics, vol. 5, no. 2, pp. 903–929, 2009.

[14] Financial Action Task Force (FATF), "Trade-Based Money Laundering," FATF Report, Paris, 2006.

[15] M. Levi and P. Reuter, "Money laundering," Crime and Justice, vol. 34, pp. 289–375, 2006.

[16] J. McSkimming, "Trade-based money laundering: Responding to an evolving threat," Journal of Money Laundering Control, vol. 19, no. 1, pp. 21–33, 2016.

[17] United Nations Office on Drugs and Crime (UNODC), "Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes," Vienna, 2011.

[18] P. Unger and M. Ferwerda, Money Laundering: A Key to Understanding Organized Crime, Corruption, and the Underground Economy, Edward Elgar Publishing, 2011.

[19] D. Ferwerda, "The effectiveness of anti–money laundering policy," Journal of Financial Crime, vol. 28, no. 3, pp. 670–689, 2021.

[20] A. Colladon and E. Remondi, "Using social network analysis to prevent money laundering," Expert Systems with Applications, vol. 67, pp. 49–58, 2017.

[21] Financial Action Task Force (FATF), "Money Laundering through the Physical Transportation of Cash," FATF Report, 2015.

[22] A. Gai, M. Lin, and D. Li, "Financial transaction fraud detection using deep learning," Neurocomputing, vol. 403, pp. 305–313, 2020.

[23] R. K. Sari, "Machine learning approaches for trade-based money laundering detection: A review," Procedia Computer Science, vol. 179, pp. 472–479, 2021.

[24] R. Rathore, Y. Sharma, P. Ambika, A. K. Upadhyay, S. Mahajan, and R. Kumar, "Data Mining Techniques in Financial Fraud Detection," Proc. IEEE 1st Int. Conf. Advances in Computing, Communication and Networking (ICAC2N 2024), pp. 1300–1305, 2024. doi: 10.1109/ICAC2N63387.2024.10895091.

[25] K. P. Sajana, S. Balan, J. Jose, and B. Kalpana, "AI-Powered Risk Management Solutions in the Banking Sector: A Data-Driven Approach," Proc. 2024 Int. Conf. Integration of Emerging Technologies for the Digital World (ICIETDW 2024), 2024. doi: 10.1109/ICIETDW61607.2024.10941397.

[26] A. Farooq and S. Selitskiy, "Data Mining Solutions for Fraud Detection in Credit Card Payments," Lecture Notes in Networks and Systems, vol. 506, pp. 880–888, 2022. doi: 10.1007/978-3-031-10461-9_60.

[27] S. Mahadik, P. Chopra, N. Kassetty, V. Ravalji, O. Goel, and J. K. Gupta, "Developing Machine Learning Models for Real-Time Fraud Detection in Online Transactions," Proc. 2025 Int. Conf. Networks and Cryptology (NETCRYPT 2025), pp. 1588–1592, 2025. doi: 10.1109/NETCRYPT65877.2025.11102173.

[28] Y. Y. Dayyabu, D. Arumugam, and S. Balasingam, "The application of artificial intelligence techniques in credit card fraud detection: A quantitative study," E3S Web of Conferences, vol. 389, art. no. 07023, 2023. doi: 10.1051/e3sconf/202338907023.

[29] S. Siddamsetti and M. Srivenkatesh, "Deep Blockchain Approach for Anomaly Detection in the Bitcoin Network," Int. J. Intelligent Systems and Applications in Engineering, vol. 12, no. 1, pp. 581–595, 2024.

[30] M. Lescano-Delgado, "Advances in the use of artificial intelligence to improve control and fraud detection in organizations," Revista Cientifica de Sistemas e Informatica, vol. 3, no. 1, art. no. e494, 2023. doi: 10.51252/rcsi.v3i1.494.

[31] M. Zhu, Y. Gong, Y. Xiang, H. Yu, and S. Huo, "Utilizing GANs for Fraud Detection: Model Training with Synthetic Transaction Data," Proc. SPIE – Int. Soc. for Optical Engineering, vol. 13180, art. no. 131803K, 2024. doi: 10.1117/12.3034346.

[32] R. A. Kumar, S. Ishrat, M. D. Prasad, P. A. Siddiq, and N. C. H. Shankar, "AI-Driven Detection Mechanism for UPI Fraud and QR Code Tampering," Proc. 6th Int. Conf. Intelligent Communication Technologies and Virtual Mobile Networks (ICICV 2025), pp. 877–883, 2025. doi: 10.1109/ICICV64824.2025.11085656.

[33] S. Gresoi, G. Stamatescu, and I. Făgărăşan, "Advanced Methodology for Fraud Detection in Energy Using Machine Learning Algorithms," Applied Sciences (Switzerland), vol. 15, no. 6, art. no. 3361, 2025. doi: 10.3390/app15063361.

[34] M. K. A. Ismaeil, "Harnessing AI for Next-Generation Financial Fraud Detection: A Data-Driven Revolution," Journal of Ecohumanism, vol. 3, no. 7, pp. 811–821, 2024. doi: 10.62754/joe.v3i7.4248.