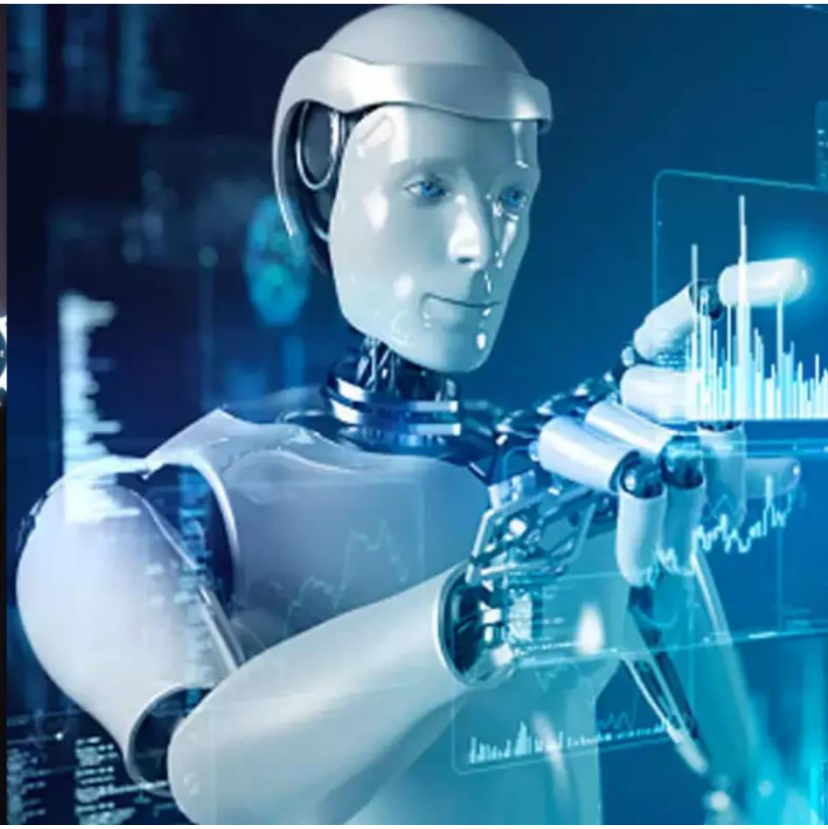
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 4, April 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404002|

AI-Driven Fraud Detection: Leveraging Machine Learning for Scam Identification

Dr. Alex Mathew, TSI Fofang

Dept. of Cybersecurity, Bethany College, USA

ABSTRACT: Fraud detection has become one of the main challenges in cybersecurity, financial security, and online shopping. Traditional rule-based fraud detection systems are no longer sufficient to struggle against ever-evolving fraud methods. Machine learning (ML) provides an adaptive, data-driven approach for detecting fraudulent activity in real time by learning patterns and detecting outliers. This article explores the main ML approaches in fraud detection: supervised learning (logistic regression, decision trees, gradient boosting, and deep learning), unsupervised learning (clustering, autoencoders, and isolation forests), and hybrid models. It also mentions the issues related to the source of the data, feature engineering, challenges such as data imbalance and concept drift, and future research directions such as explainable AI, adversarial machine learning defenses, and real-time fraud detection using Edge AI. The result indicates that fraud detection based on AI greatly enhances accuracy, scalability, and adaptability and is, hence, a critical tool in modern-day cybersecurity.

KEYWORDS: Fraud detection, machine learning, anomaly detection, cybersecurity, supervised learning, unsupervised learning, AI-driven security.

I. INTRODUCTION

With the rise in online payments, fraud has grown in the banking, e-commerce, and telecom sectors (Odufisan et al., 2025). Fraudsters constantly develop new methods that rule-based fraud detection systems cannot detect. These systems work based on known patterns and cannot detect new dynamically changing fraud methods (Njoku et al., 2024). To address this issue, machine learning and artificial intelligence have emerged as powerful tools to detect fraudulent activity in real time (Bello & Olufemi, 2024). Machine learning algorithms offer fraud detection using a data-driven approach by processing large datasets, learning patterns, and identifying outliers. Unlike static rule-based systems, ML models constantly learn to adapt to new fraud techniques and provide increased detection accuracy (Shihembetsa, 2021). Herein, we present important machine-learning approaches in fraud detection, including supervised, unsupervised, and hybrid models. We also address the source of the data, feature engineering, and the limitations of fraud detection using AI and provide fraud prevention directions for the future.

II. KEY MACHINE LEARNING TECHNIQUES FOR FRAUD DETECTION

Supervised Learning Methods (Labeled Data Available)

Supervised learning requires labeled datasets in which the fraudulent and legitimate transactions are known. They learn from the history and predict whether new transactions are fraudulent (Afriyie et al., 2023). A very simple yet very powerful supervised learning approach is the application of logistic regression for classifying fraudulent and genuine transactions. Although the disadvantage of logistic regression is that it does not work well for complex fraud patterns, decision trees and random forests address this by classifying the transaction based on a collection of decision rules (International, 2022). Random forests enhance this by using multiple decision trees to provide better accuracy.

More advanced boosting techniques like Gradient Boosting Machines (GBM) and XGBoost improve fraud detection by iteratively correcting misclassified samples (Olushola & Mart, 2024). These models also detect subtle fraud patterns by assigning specific weights to specific features. Deep learning-based neural networks work well in large datasets and sophisticated fraud patterns that might evade regular models. Neural networks can detect complex fraud patterns and complex fraudulent transactional dependencies and are very effective in today's fraud detection systems.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404002|

Figure 1: Decision Tree Structure (Supervised Learning)

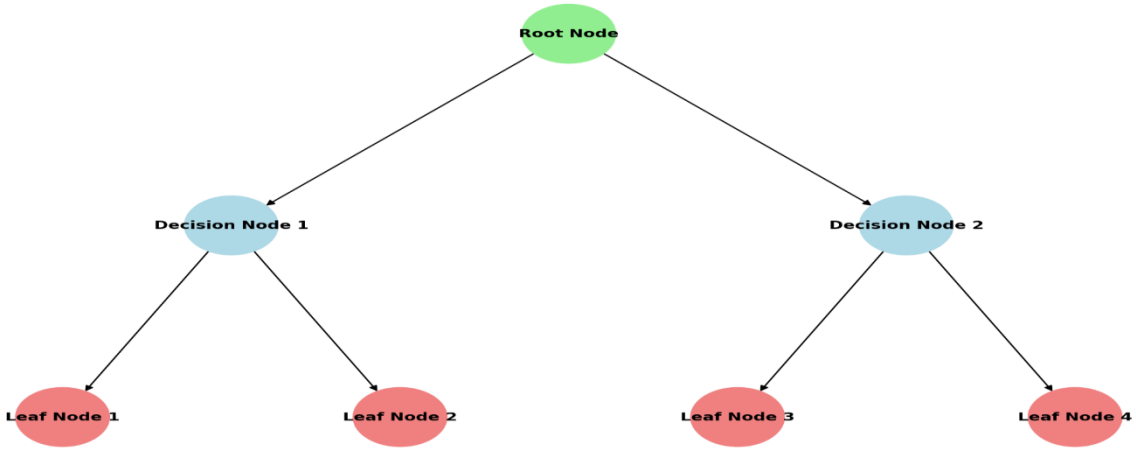


Figure 1: Supervised Learning

Unsupervised Learning Methods (Anomaly Detection)

Unsupervised learning has particular use in fraud detection since fraud itself happens comparatively infrequently, and thus, labeled data sets are not straightforward to acquire. Such models detect fraud by searching for deviations from normal transactional activity (Bello et al., 2023). Clustering algorithms such as K-Means and DBSCAN detect similar transactions and outliers as potential fraud instances. These models detect outliers by observing transaction clusters and identifying deviations from normal user behavior. Autoencoders, being neural networks, learn normal transaction behaviors and identify any deviations as suspect (Cédric Poutré et al., 2024). Since they are trained on non-fraudulent transaction reconstruction, any deviation from normal transaction behavior is flagged as an anomaly. Isolation forests, another anomaly detection technique that has become very popular, isolate the anomaly by randomly choosing features and partitioning the data. Since fraud transactions are rare in number, they are isolated earlier in the tree development process.

Figure 2: Unsupervised Anomaly Detection Methods

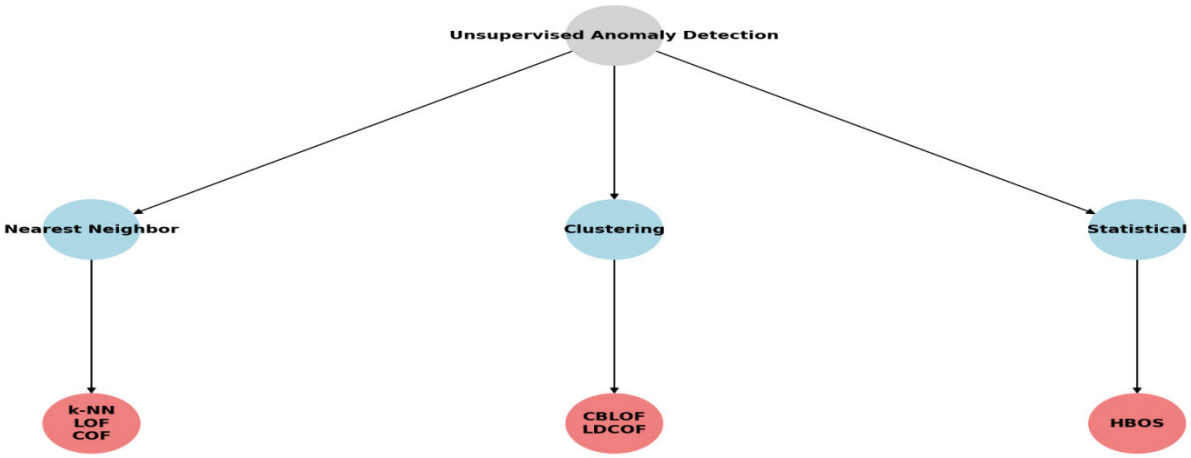


Figure 2: Unsupervised Learning

Hybrid and Ensemble Models

Hybrid models employ supervised and unsupervised learning to enhance the effectiveness of fraud detection. Employing an autoencoder for anomaly detection and feeding the suspicious transactions to an XGBoost classifier for analysis is a common approach. The approach reduces the false positives and enhances fraud detection (Saini et al.,

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404002|

2023). Ensemble models, which combine multiple algorithms, enhance fraud detection further by leveraging the strengths of the different approaches.

III. PROPOSED METHODOLOGY

Data Gathering Sources

Fraud detection models require more than one source of data to determine fraudulent transactions. One of them is the records of transactions of financial transactions, like credit card transactions, wire transfers of banks, and online payments (Cherif et al., 2022). E-commerce records, including fraudulent orders, fake reviews, and account takeovers, also provide useful information (Ayorinde, 2021). Fraud detection in social media and email records, where the most common types include phishing and impersonation fraud, is another important area. Telecommunication records, including robocalls and SMS fraud, also assist in identifying fraudulent activity.

Feature Engineering for Fraud Detection

Feature engineering is essential in the improvement of the performance of ML models by extracting useful information from raw data (Ikeda et al., 2021).

- **Transaction-Based Features:** These are transaction amount, frequency, location, and time of the transaction, which are used to detect unusual spending behavior.
- **User Behavior Analysis:** Frequency of login, spending pattern, and the device utilized provide indicators of potential fraud incidents. Unusual behavior, such as login attempts from unfamiliar devices or spending bursts, indicates fraud (Ti et al., 2022).
- **Text analysis for Scam Detection:** Natural Language Processing-based approaches analyze scam-specific terms, sentiment patterns, and linguistic indicators within emails and messages.
- **Graph-Based Features:** Scammers operate in fraudulent account networks. Graph-based models analyze the relationship between the accounts belonging to the scammers and detect organized fraud rings.

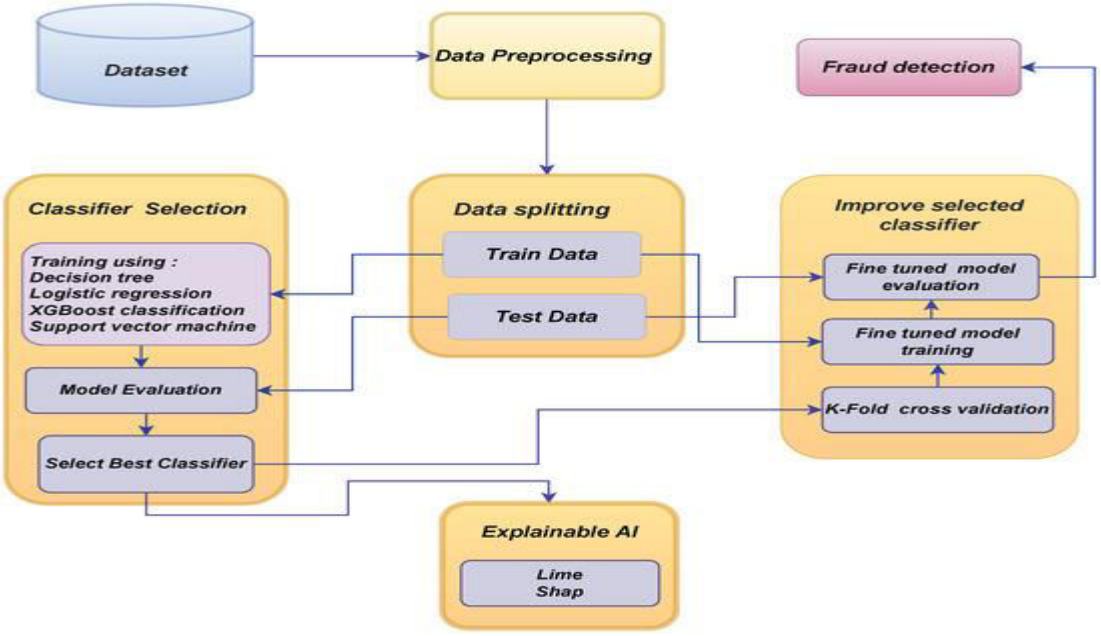


Figure 3: Feature of Unmasking Fraud

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404002|

Figure 4: Machine Learning Module Workflow

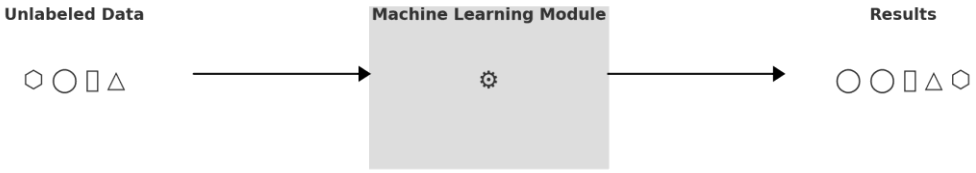


Figure 4: Algorithm of Risk Management

Model Training & Evaluation

Fraud detection models face the issue of class imbalance since fraud attempts are rare compared to legitimate ones. Synthetic Minority Over-sampling Technique (SMOTE) solves the issue by balancing the dataset. Concept drift—perpetual strategy changes by the scammers—also requires the models to be retrained constantly. Model accuracy is gauged by precision, recall, and F1-score. Accuracy must be weighed against false positives to avoid blocking genuine users.

IV. RESULTS AND ANALYSIS

Effectiveness of AI-Driven Fraud Detection

Fraud detection models using AI are significantly better than traditional rule-based systems. Supervised models such as random forests and XGBoost work well when labeled samples are used (Aryan Ananya et al., 2025). However, unsupervised models such as autoencoders and isolation forests are better suited for detecting new fraud patterns. Hybrid models offer the optimal balance between the two by integrating anomaly detection and classification methods for enhanced fraud prevention.

V. REAL-WORLD APPLICATIONS AND CASE STUDIES

- **Banking & Fintech:** Banks like Visa and PayPal use ML to process payments and detect real-time fraud.
- **E-commerce websites:** Amazon and eBay utilize AI to identify counterfeit reviews and fake seller activity.
- **Cryptocurrency Exchanges:** Binance and Coinbase both use AI to prevent money laundering and fraud.
- **Social media websites:** Facebook and Twitter use machine learning to identify fake accounts, spam messages, and impersonate scams.

VI. PROBLEMS IN FRAUD DETECTION USING AI

Although effective, fraud detection using AI has numerous challenges. Data imbalance is another issue because fraud activity is rare, and the models cannot learn effectively (Adhikari et al., 2024). Concept drift also requires models to be retrained continuously because fraudsters adapt over the years. Explainability and interpretability are concerns, particularly for deep learning "black box" models. Models must be transparent and interpretable for regulatory requirements. False positives are also troublesome because fraud detection systems that are too aggressive can inconvenience legitimate clients.

VII. CONCLUSION & FUTURE RESEARCH DIRECTIONS

Machine learning has transformed fraud detection by providing adaptive and data-driven approaches that are better than traditional methods (Snezana et al., 2025). Future research needs to focus on federated learning that will enable multiple institutions to train fraud detection models without sharing sensitive information. Explainable AI (XAI) will increase the transparency of models, and adversarial ML defenses will make fraud detection more robust against cyber criminals (Bello et al., 2024). Real-time fraud detection based on Edge AI will also enable fraud prevention on mobile. With continuous advancements in AI, fraud detection will become increasingly effective in mitigating financial fraud and cybercrime.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404002|

REFERENCES

1. Adhikari, P., Hamal, P., & Jnr, F. B. (2024). Artificial Intelligence in fraud detection: Revolutionizing financial security. International Journal of Science and Research Archive, 13(1), 1457–1472. https://doi.org/10.30574/ijsra.2024.13.1.1860
2. Afriyie, J. K., Tawiah, K., Pels, W. A., Addai-Henne, S., Dwamena, H. A., Owiredu, E. O., Ayeh, S. A., & Eshun, J. (2023). A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions. Decision Analytics Journal, 6(100163), 100163. https://doi.org/10.1016/j.dajour.2023.100163
3. Aryan Ananya, Vikram Shreya, Aditya Neha, Saanvi Deepika, & Falade rhoda Adeola. (2025). The Role of AI and Machine Learning in Fraud Detection for Digital Banking. https://www.researchgate.net/publication/388566383_The_Role_of_AI_and_Machine_Learning_in_Fraud_Detection_for_Digital_Banking
4. Ayorinde, K. (2021). Cornerstone: A Collection of Scholarly Cornerstone: A Collection of Scholarly and Creative Works for Minnesota and Creative Works for A Methodology for Detecting Credit Card Fraud A Methodology for Detecting Credit Card Fraud. https://cornerstone.lib.mnsu.edu/cgi/viewcontent.cgi?article=2167&context=etds
5. Bello, A., & Olufemi, K. (2024). Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities. Computer Science & IT Research Journal, 5(6), 1505–1520. https://doi.org/10.51594/csitrj.v5i6.1252
6. Bello, O., Folorunso, A., Ejiofor, O., Zainab Budale, F., Adebayo, K., Olayemi, A., Babatunde, & Bello, C. (2023). Machine Learning Approaches for Enhancing Fraud Prevention in Financial Transactions. International Journal of Management Technology, 10(1), 85–109. https://doi.org/10.37745/ijmt.2013/vol10n185109
7. Bello, O., None Courage Idemudia, & Iyelolu, V. (2024). Implementing machine learning algorithms to detect and prevent financial fraud in real-time. Computer Science & IT Research Journal, 5(7), 1539–1564. https://doi.org/10.51594/csitrj.v5i7.1274
8. Cédric Poutré, Didier Chételat, & Morales, M. (2024). Deep Unsupervised Anomaly Detection in High-Frequency Markets. ˜ the œJournal of Finance and Data Science, 100129–100129. https://doi.org/10.1016/j.jfds.2024.100129
9. Cherif, A., Badhib, A., Ammar, H., Alshehri, S., Kalkatawi, M., & Imine, A. (2022). Credit card fraud detection in the era of disruptive technologies: A systematic review. Journal of King Saud University - Computer and Information Sciences, 35(1). https://doi.org/10.1016/j.jksuci.2022.11.008
10. Ikeda, C., Ouazzane, K., Yu, Q., & Hubenova, S. (2021). New Feature Engineering Framework for Deep Learning in Financial Fraud Detection. International Journal of Advanced Computer Science and Applications, 12(12). https://doi.org/10.14569/ijacsa.2021.0121202
11. International, F. (2022). The advantages of Machine Learning in Fraud Prevention. Fraud.com. https://www.fraud.com/post/the-advantages-of-machine-learning-in-fraud-prevention
12. Njoku, D. O., Vitalis Chibuike Iwuchukwu, Jibiri, J. E., & Nwokoma, F. O. (2024). Machine Learning Approach for Fraud Detection System in Financial Institution: A Web Base Application. ResearchGate. https://www.researchgate.net/publication/380174951_Machine_Learning_Approach_for_Fraud_Detection_System_in_Financial_Institution_A_Web_Base_Application
13. Odufisan, O. I., Abhulimen, O. V., & Ogunti, E. Olarenwaju. (2025). Harnessing Artificial Intelligence and Machine Learning for Fraud Detection and Prevention in Nigeria. Journal of Economic Criminology, 100127. https://doi.org/10.1016/j.jeconc.2025.100127
14. Olushola, A., & Mart, J. (2024). Fraud Detection using Machine Learning. World Journal of Advanced Research and Reviews. https://doi.org/10.14293/pr2199.000647.v1
15. Saini, N., Vivekananda Bhat Kasaragod, Prakash, K., & Ashok Kumar Das. (2023). A hybrid ensemble machine learning model for detecting APT attacks based on network behavior anomaly detection. Concurrency and Computation: Practice and Experience. https://doi.org/10.1002/cpe.7865
16. Shihembetsa, E. (2021). USE OF ARTIFICIAL INTELLIGENCE ALGORITHMS TO ENHANCE FRAUD DETECTION IN THE BANKING INDUSTRY. https://erepository.uonbi.ac.ke/bitstream/handle/11295/155920/Shihembetsa_Use%20of%20artificial%20intelligence%20algorithms%20to%20enhance%20fraud%20detection%20in%20the%20Banking%20Industry.pdf?sequence=1
17. Snezana, A., Polina, H., Platon Viktoriya, & Adebayo, H. (2025, February). The Evolution of Machine Learning in Financial Fraud Detection. ResearchGate; unknown.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404002|

https://www.researchgate.net/publication/388585383_The_Evolution_of_Machine_Learning_in_Financial_Fraud_Detection

18. Ti, Y.-W., Hsin, Y.-Y., Dai, T.-S., Huang, M.-C., & Liu, L.-C. (2022). Feature generation and contribution comparison for electronic fraud detection. Scientific Reports, 12(1), 18042. https://doi.org/10.1038/s41598-022-22130-2
19. Nobel, N., Sultana, S., Sondip Poul Singha, Sudipto Chaki, Mahi, N., Jan, T., Barros, A., & Md Whaiduzzaman. (2024). Unmasking Banking Fraud: Unleashing the Power of Machine Learning and Explainable AI (XAI) on Imbalanced Data. Information, 15(6), 298–298. https://doi.org/10.3390/info15060298

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details