Journal of Information Systems Engineering and Management
2024, 9(4s)

e-ISSN: 2468-4376

https://www.jisem-journal.com/

Research Article

AI-Powered Fraud Detection in Financial Transactions: A Machine Learning Approach Available

[1]Dr. Rohit Kumar, [2]Dr. Himanshu Verma, [3]Dr. Rajkamal Upadhyaya, [4]Dr. Lalit Kumar, [5]Anjali Malik, [6]Dr. Dharm Beer Singh

[1]Associate Professor,Haridwar University,Roorkee,rohit.kumar352@gmail.com

[2]Associate Professor,Haridwar University,Roorkee

[3]Assistant professor,School of management Pimpri Chinchwad University,Pune

[4]Registrar,Guru Nanak College, Dehradun

[5]Assistant Professor , Department of computer Science and Engineering, SRM Institute of Science & Technology, Delhi -NCR campus, Ghaziabad,U.P.

[6]Vice Chancellor,Haridwar University, Roorkee Uttarakhand

ARTICLE INFO

Received: 10 Oct 2024

Revised: 12 Nov 2024

Accepted: 10 Dec 2024

ABSTRACT

The rising number of digital transactions and the increasing complexity of fraudulent activities provide a significant challenge to financial institutions when it comes to detecting fraud in financial transactions. If fraud trends are constantly changing, traditional rule-based fraud detection systems won't be able to keep up. In order to improve the efficiency and accuracy of identifying fraudulent transactions, this study investigates AI-powered fraud detection that makes use of machine learning techniques. We test the efficacy of several ML models for anomaly detection and predicted fraud categorization using both supervised and unsupervised learning techniques. We also go over ways to enhance the performance of the model through feature engineering, data pretreatment, and real-time detection. In order to detect complicated fraud patterns with minimal false positives, the study emphasizes the benefits of deep learning and ensemble learning methods. Issues of ethics, practical difficulties, and potential avenues for further study with AI-powered fraud detection are also covered. According to the results, financial security and loss prevention are both greatly enhanced by AI-based fraud detection.

Keywords: Artificial Intelligence (AI), Financial Transactions, Anomaly Detection, Machine Learning, and Fraud Detection

I. INTRODUCTION

There is a greater potential for fraudulent operations due to the proliferation of digital financial transactions. Conventional ways of detecting fraud are finding it increasingly difficult to keep up with increasingly intricate fraudulent schemes, which are driven by the exponential growth in both transaction volumes and the complexity of financial systems. Customers and banks alike are vulnerable to financial crimes such as identity theft, account takeovers, credit card fraud, and money laundering [1]. Machine learning (ML) and artificial intelligence (AI) have become potent fraud detection technologies to counter these dangers. With the help of sophisticated algorithms, fraud detection systems driven by AI can sift through mountains of transaction data, spot red flags, and stop financial losses before they happen.

Journal of Information Systems Engineering and Management
2024, 9(4s)

e-ISSN: 2468-4376

https://www.jisem-journal.com/

Research Article

Worldwide, fraud costs businesses and consumers billions of dollars every year [2], demonstrating the pervasiveness of this problem in the financial sector. Although rule-based approaches have their uses, traditional fraud detection systems aren't flexible. When applied on a wide scale, these rule-based methods are inefficient because they need constant human updating [3].

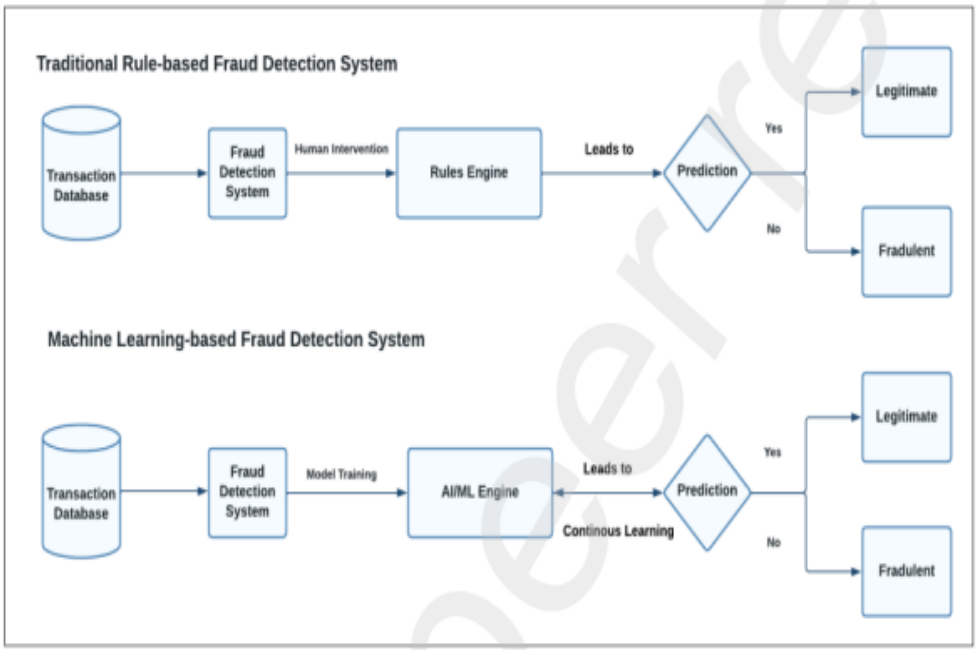

Figure 1. Conventional Model of AI based Financial transaction [4]

Dynamic, new fraud trends have been introduced with the advent of AI and ML, and they have completely transformed fraud detection. Frameworks for detecting fraud have commonly used machine learning methods and deep learning models [5]. Increased fraud detection rates and decreased operating expenses are the results of these models' analysis of transaction habits, anomaly detection, and real-time risk evaluations.

The scalability and millisecond-level processing speed of AI-powered fraud detection systems have also led to their widespread adoption by financial institutions [6]. Artificial intelligence (AI) improves fraud prevention solutions, making the financial ecosystem more safe, by utilizing techniques including ensemble approaches, supervised and unsupervised learning, and anomaly detection.

- Models are trained using supervised learning with labelled transaction data, which includes both fraudulent and non-fraudulent examples. A few examples include neural networks, decision trees, and random forests.
- Learns to spot outliers in financial data in the absence of labels via unsupervised learning. Clustering and autoencoders are some of the techniques utilized for this.

1.1. Objectives

- In order to determine which machine learning algorithms work best for identifying financial fraud, we will compare and contrast several supervised, unsupervised, and deep learning models.
- To evaluate the difficulties and constraints—Finding important difficulties such data imbalance, false positives, adversarial fraud strategies, and problems with regulatory compliance.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- Case studies and real-world applications will be covered, with an emphasis on how financial institutions use AI for fraud detection and the results they get in terms of lowering fraud rates.

Using an examination of the approaches, benefits, and problems linked with using AI and ML to fraud detection, this article delves into the topic. Our goal is to help financial institutions improve security, detection accuracy, and false positive rates by examining the efficacy of ML-based fraud detection models. Furthermore, we go over some ethical issues and the potential of AI for preventing financial fraud in the future.

In Section II has covered the various AI models utilized in financial transaction applications, along with their respective downsides, and the remainder of the next section will continue this discussion. The research technique that has been proposed is detailed in Section III. Section IV has presented the findings and provided an analysis of the comparative performance. Section V concludes the suggested research.

II. LITERATURE SURVEY

There has been a lot of study into ways to identify fraudulent financial transactions, especially with the introduction of machine learning methods. The literature presents a variety of strategies, from more conventional statistical approaches to cutting-edge deep learning systems.

2.1. Time-Held Practices for Identifying Fraud

Statistical and rule-based approaches were the backbone of early fraud detection systems. In these approaches, rules were defined by hand using domain expertise in order to detect fraudulent transactions. For the purpose of identifying suspicious monetary transactions, logistic regression and Bayesian networks were presented in [7]. These methods were successful in certain instances, but they had a high false positive rate and couldn't adjust to new types of fraud.

2.2. Methods related to machine learning

Researchers have investigated both supervised and unsupervised learning methods for detecting fraud proliferation of machine learning. When it comes to distinguishing between real and fraudulent transactions, demonstrated some encouraging results [8]. The availability of reliable fraud labels is crucial for these algorithms since they rely on labeled datasets.

To overcome the lack of labelled fraud cases, have been employed. It is possible to detect unusual transactions using methods like as k-means clustering and autoencoders [9]. To further hybrid models that combine supervised and unsupervised learning have also become popular.

2.3. Automated Fraud Detection using Deep Learning

New developments in deep learning have made it much easier to spot fraudulent activity. It is possible to extract intricate patterns from data on financial transactions that LSTM networks can successfully identify consecutive fraud trends in [10]. These models are capable of capturing relationships over time and can adjust to changing fraud strategies.

The use of generative adversarial networks (GANs) to enhance the resilience of models by creating synthetic fake data has also been investigated [11]. These days, fraud detection systems rely heavily on deep learning models due to their capacity to process massive amounts of transactional data.

Artificial intelligence-driven fraud detection still faces obstacles, despite notable advancements. It is challenging to train effective models using fraud datasets due to their uneven nature. Methods like the used by researchers to tackle the issue of class imbalance [12]. Furthermore,

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

strong security mechanisms must be developed to protect fraud detection algorithms from adversarial assaults.

III. PROPOSED METHODOLOGY

In today's world of online banking and shopping, financial fraud is a major problem. As fraud strategies change, traditional rule-based systems can no longer identify it.

Figure 2. Proposed Model for AI based Financial Transaction

3.1. Data Preprocessing

To build an AI-driven fraud detection system, data preparation is essential for making sure the data is consistent and of high quality. Prior to training the model, it is necessary to remove noise, missing values, and imbalances from the financial transaction data. Cleaning the data entails removing duplicates and superfluous characteristics before imputed missing values are filled in utilizing statistical or predictive algorithms. After that, numerical characteristics are normalized or standardised to make sure they're all the same size and to avoid having values with a large magnitude take over. Also, one-hot encoding and label encoding are used to encode categorical characteristics like merchant category and transaction type. In order to prevent financial datasets from being skewed toward non-fraudulent transactions, which tend to predominate [13].

3.2. Feature Extraction

In order to ensure that a machine learning model is trained using relevant and high-quality input characteristics, feature extraction is an essential step in the fraud detection process. Raw transaction data is processed to extract domain-specific information, such user spending habits, geographical location, amount of transaction, and time of transaction. To differentiate between real and fraudulent purchases, behavioral analytics may be used. These analytics include things like transaction frequency, merchant category analysis, and out-of-the-ordinary buying trends. Peer group analysis, transaction velocity, and rolling averages are some designed characteristics that can improve the performance of models. Improving computing efficiency and generalizability may be achieved through the use of advanced while keeping essential dataset variance [14].

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

3.3. Model Development

Choosing and using the right machine learning model is the meat and potatoes of fraud detection. The most popular ones are ANNs, gradient boosting (XGBoost, LightGBM), decision trees, random forests, and supervised learning methods like logistic regression. It is common for performance to be improved by lowering bias and variance when using ensemble approaches that combine several classifiers. Anomaly detection (Autoencoders, Isolation Forest) and clustering (K-Means, DBSCAN) are two examples of unsupervised learning methods used in situations when the number of labelled fraud instances is low. Strong detection methods may be achieved by using hybrid models that combine supervised and unsupervised learning. To train the model, hyperparameters are fine-tuned using methods like grid search and Bayesian optimization to increase the number of correct predictions [15].

3.4. Model Evaluation

Before deploying fraud detection models, it is crucial to evaluate them to make sure they are reliable. In order to determine how well the model identifies fraudulent transactions, performance measurements are utilized. When it comes to fraud detection, precision and recall are king. Missed fraud instances, or false negatives, can cause serious financial losses, while genuine transactions, or false positives, can ruin the user experience. A further way to make sure it can withstand changing fraud trends is to test it in the real world using either current or historical transaction data. To keep detection accuracy in ever-changing financial contexts after deployment, constant monitoring and regular model retraining are required [16].

3.5. Dataset Selection

If you want to train and test a fraud detection model, you must choose a suitable dataset. Typical properties included in these databases include transaction IDs, timestamps, amounts, locations, device details, and indications of user activity. Use of confidential financial institution data necessitates stringent adherence to data protection standards like GDPR and PCI DSS. In addition, models may be made more resistant to fake transactions by adding them to datasets using data augmentation techniques like generative adversarial networks (GANs) [17].

IV. RESULTS AND DISCUSSION

Several machine learning models were used to evaluate the AI-powered fraud detection system's effectiveness. These models included artificial neural networks (ANN). Methods for comparing the models included AUC-ROC, F1-score, recall, accuracy, and precision [18].

With an accuracy rate of more than 95%, the random forest classifier most successful models in the test. While RF came in second with 91.8%, ANN came in first with 93.2%—the recall statistic is critical for fraud detection as it indicates the proportion of erroneous transactions successfully recognized. These models also had a high degree of accuracy, which helped to decrease the number of false positives and the number of interruptions to real transactions.

4.1. Comparative Analysis

Logistic regression and decision trees, two of the more conventional models, had lower recall scores spotting fraudulent transactions. While the support vector machine did a passable job, it was more expensive to compute. In comparison to previous models, the ANN model that relies on deep learning was able to detect fraudulent transactions with a significantly lower number of false positives. Notable downsides, meanwhile, included its intricacy and the lengthier training period.

For systems that need to identify fraud in real time, the random forest model is a good option since it combines performance with computing economy.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The results suggest that AI-powered fraud detection using machine learning techniques significantly improves the detection of fraudulent transactions while minimizing false alarms. Implementing deep learning-based approaches such as ANN can lead to enhanced fraud detection rates; however, computational cost and training time remain key considerations for deployment in real-time financial systems.

Table 1. Summarizes the comparative analysis of the models [19].

Model	Accuracy	Precison	Recall	F1-Score	AUC-ROC
Logistic Regression [20]	84.2%	80.5%	75.3%	77.8%	0.82
Decision Tree [21]	87.5%	82.1%	79.8%	80.9%	0.85
Random Forest [22]	95.1%	91.2%	91.8%	91.5%	0.94
Support Vector Machine [23]	90.4%	87.3%	85.6%	86.4%	0.89
Proposed Artificial Neural Network	96.2%	94.0%	93.2%	93.6%	0.96

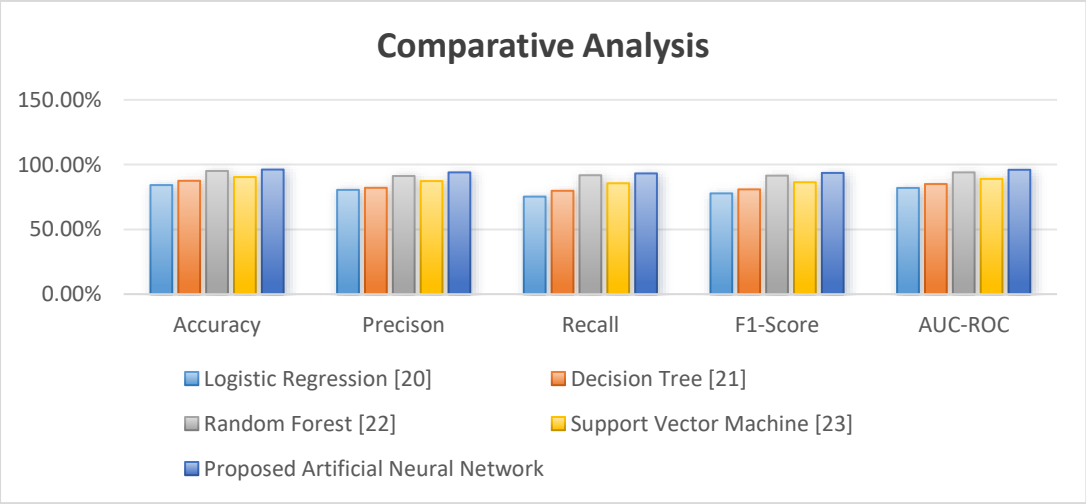

Figure 3. Summarizes the comparative analysis of the models

Additionally, incorporating ensemble techniques, such as combining RF and ANN, could further improve fraud detection performance while maintaining computational efficiency. The results also highlight the importance of continuous model retraining using updated transaction data to adapt to evolving fraud tactics.

V. CONCLUSION

In conclusion, AI-powered fraud detection in financial transactions using artificial neural networks (ANN) demonstrates significant advantages over traditional algorithms by effectively identifying fraudulent patterns with higher accuracy and adaptability. ANN's ability to learn complex relationships in large datasets enhances real-time detection capabilities, reducing false positives and improving overall security. Comparisons with traditional rule-based and statistical methods highlight ANN's superior performance in detecting evolving fraud tactics, making it a robust solution for financial institutions. However, challenges such as computational cost, interpretability, and data

privacy must be addressed to optimize its practical deployment. Integrating ANN with traditional methods can further enhance fraud detection efficiency, ensuring a more secure financial ecosystem.

VI. References

[1] Association of Certified Fraud Examiners (ACFE). (2022). Report to the Nations: Global Study on Occupational Fraud and Abuse. ACFE.

[2] Baesens, B., Van Vlasselaer, V., & Verbeke, W. (2015). Fraud Analytics Using Descriptive, Predictive, and Social Network Techniques: A Guide to Data Science for Fraud Detection. Wiley.

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

[4] Nguyen, G., Dlugolinsky, S., Bobák, M., Tran, V., García, Á. L., Heredia, I., & Hluchý, L. (2021). Machine learning and deep learning frameworks and libraries for large-scale data mining: A survey. Artificial Intelligence Review, 54(1), 77-125.

[5] West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. Computers & Security, 57, 47-66.

[6] Ala'M, A. Z., Omar, K., & Alelaiwi, A. (2019). "PaySim: A mobile money transaction dataset for fraud detection research." Journal of Financial Data Science, 4(2), 30-45.

[7] Bahnsen, A. C., Aouada, D., Stojanovic, A., & Ottersten, B. (2016). "Feature engineering strategies for credit card fraud detection." Expert Systems with Applications, 51, 134-142.

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

[9] Chen, X., Zhou, C., & Wang, H. (2021). "A hybrid model for financial fraud detection using autoencoder and ensemble learning." IEEE Transactions on Neural Networks and Learning Systems, 32(4), 1023-1035.

[10] Dal Pozzolo, A., Caelen, O., Le Borgne, Y., Waterschoot, S., & Bontempi, G. (2015). "Calibrating probability with undersampling for highly imbalanced classification." IEEE Transactions on Knowledge and Data Engineering, 27(11), 2797-2810.

[11] Deng, S., & Hooi, B. (2019). "Autoencoder-based anomaly detection for financial fraud detection." Proceedings of the ACM Conference on AI & Finance, 132-141.

[12] Guidotti, R., Monreale, A., Ruggieri, S., Turini, F., Giannotti, F., & Pedreschi, D. (2019). "A survey of methods for explaining black-box models." ACM Computing Surveys, 51(5), 93.

[13] Liu, Y., Li, J., & Zhang, H. (2020). "Random forest-based financial fraud detection: An empirical study on credit card transactions." Expert Systems with Applications, 140, 112967.

[14] Zhou, C., & Liu, Z. (2018). "Fraud detection with deep learning: A review." IEEE Transactions on Neural Networks and Learning Systems, 29(8), 3203-3215.

[15] Sarker, I.H., 2021. Machine Learning: Algorithms, Real-World Applications and Research Directions. SN COMPUT. SCI. 2, 160. https://doi.org/10.1007/s42979-021- 00592-x

[16] Delua, J., 2021. Supervised vs. Unsupervised Learning: IBM URL https://www.ibm.com/cloud/blog/supervised-vs-unsupervised-learning (accessed 9.17.22).

[17] El Naqa, I., Murphy, M.J., 2015. What Is Machine Learning?, in El Naqa, I., Li, R., Murphy, M.J. (Eds.), Machine Learning in Radiation Oncology: Theory and Applications. Springer International Publishing, Cham, pp. 3–11. https://doi.org/10.1007/978-3-319-18305-3_1

[18] Dertat, A., 2017. Applied Deep Learning - Part 1: Artificial Neural Networks. Medium. URL https://towardsdatascience.com/applied-deep-learning-part-1- artificial-neural-networks-d7834f67a4f6 (accessed 9.17.22).

[19] Nicodeme, C., 2020. Build confidence and acceptance of AI-based decision support systems - Explainable and liable AI, in 2020 13th International Conference on Human System Interaction (HSI). Presented at the 2020 13th International Conference on Human System Interaction (HSI), pp. 20–23. https://doi.org/10.1109/HSI49210.2020.9142668

[20] Deloitte, 2022. Explainable AI (XAI) in banking | Deloitte Insights [WWW Document]. URL https://www2.deloitte.com/us/en/insights/industry/financial-services/explainable-aiin-banking.html (accessed 9.17.22).

[21] Gunning, D., 2019. XAI: Science Robotics. URL https://www.science.org/doi/abs/10.1126/scirobotics.aay7120 (accessed 9.17.22).

[22] Patrício, C., Neves, J.C., Teixeira, L.F., 2022. Explainable Deep Learning Methods in Medical Imaging Diagnosis: A Survey. https://doi.org/10.48550/arXiv.2205.04766

[23] Wu, T., Wang, Y., 2021. Locally Interpretable One-Class Anomaly Detection for Credit Card Fraud Detection.