The American Journal of Applied Sciences

ISSN 2689-0992 | Open Access

TYPE Original Research
PAGE NO. 128-132
DOI 10.37547/tajas/Volume07Issue07-13

Comparing Neural Networks and Traditional Algorithms in Fraud Detection

Dip Bharatbhai Patel
University of North America, Virginia, USA

OPEN ACCESS

SUBMITED 18 June 2025
ACCEPTED 24 June 2025
PUBLISHED 27 July 2025
VOLUME Vol.07 Issue 07 2025

CITATION
Dip Bharatbhai Patel. (2025). Comparing Neural Networks and Traditional Algorithms in Fraud Detection. The American Journal of Applied Sciences, 7(07), 128–132. https://doi.org/10.37547/tajas/Volume07Issue07-13

Abstract: Fraud detection has become an essential component of financial security systems. Traditional algorithms have long served as the backbone of these systems. The rise of neural networks is revolutionizing the process as it offers new approaches to identifying complex fraud patterns. The paper presents a comparative analysis of neural networks and traditional algorithms. These include decision trees, rule-based systems, and logistic regression in fraud detection. The comparison is based on scalability, accuracy, interpretability, computational efficiency, and adaptability. The findings reveal that neural networks outperform traditional methods in subtle, non-linear fraud patterns but suffer from interpretability and data requirements. A hybrid detection framework that combines neural intelligence with rule-based logic is proposed for real-time, robust fraud management. For instance, a neural ensemble model achieved over 97% accuracy while traditional systems achieved 89-91%. The paper highlights that the hybrid approach offers optimal results in real-world scenarios.

Keywords: Fraud detection, neural networks, machine learning, traditional algorithms, anomaly detection.

I. INTRODUCTION

Fraud poses a significant threat to global financial systems. It is costing many companies billions annually. As digital transactions increase, the complexity of fraudulent behaviors also increases. Therefore, fraud detection systems must evolve to detect and identify fraudsters' ever-changing tactics. Historically, traditional algorithms have served as the key detection mechanism. However, neural networks and deep learning have emerged as the most effective tools in predictive analytics and anomaly detection. Traditional machine learning techniques like decision trees, support vector machines, and logistic regression are widely used due to their transparency, and they are easy to deploy. Neural networks have revolutionized the field of pattern recognition and anomaly detection. It is capable of learning complex temporal, behavioral, and spatial patterns. This strategy is effective in adapting to fraud tactics that escape traditional logic.

Despite these strengths, neural models are often criticized for their "black box" nature and computational complexity. The paper compares traditional algorithms and neural networks to determine their strengths and weaknesses in fraud detection. It will explore how each method works, analyze performance metrics, and assess their practicality in real-world applications.

II. Literature Review

Fraud detection involves identifying suspicious or unauthorized transactions within massive datasets. Techniques used can be categorized into classifications, which are supervised. We have unsupervised, which is anomaly detection. Traditional methods like decision trees, support vector machines, and logistic regression rely on predefined rules and feature engineering. Neural networks, such as deep learning models, leverage hierarchical layers to learn complex data representations.

Many issues are encountered by fraud detection systems, including evolving fraud patterns, class imbalance, and the need for real-time detection. Therefore, it is essential to select the correct algorithm to handle these challenges effectively.

A. Traditional Fraud Detection Algorithms

These algorithms have long been employed in fraud detection due to their interpretability, ease of implementation, and simplicity. Logistic regression is one of the most commonly used techniques. It is effective due to its speed and ability to handle binary classification. This approach assumes a linear relationship and struggles with complex patterns. Another method is decision trees and random forests. The models are intuitive and can handle non-linear data better than regression. Random forest, for instance, can improve performance via ensemble learning (Murorunkwere et al., 2022). The model might be computationally expensive on large datasets. We have Rule-based systems that heavily rely on domain expertise. Rule-based systems are critical to providing transparent decisions. However, these models are brittle and demand frequent updates to match the ever-changing fraud patterns.

Okur et al. (2021) believe the Support Vector Machine (SVM) model is effective in high-dimensional spaces. They are used in linear and non-linear classification. However, they have limitations, such as handling large-scale datasets. These authors discovered that rule-based and statistical models like decision SVM and decision trees are still being used extensively. Their simplicity allows for rapid deployment and transparency. They, however, limit adaptability to changing fraud trends.

B. Neural Networks for Fraud Detection

Neural networks, intense learning models such as RNNs and CNNs, improve fraud detection accuracy. They are capable of automatically learning hierarchical data patterns. Osegi and Jumbo (2021) propose a simulated annealing-trained neural model outperforming traditional classifiers.

Artificial Neural Networks (ANNs)

These networks mimic brain-like structures, and they can handle complex non-linear relationships. These models are effective when they are well-trained on large datasets. These datasets must be well-labeled to make it easy to operate.

Convolutional Neural Networks (CNNs)

These models are standard in image processing. These models can also be used for feature extraction in traditional patterns and are effective in user behaviors (Okur et al., 2021).

Recurrent Neural Networks (RNNs) and LSTMs

These models are well-suited for sequential data like transaction time series. The models offer various advantages, like tracking behavioral anomalies over time, which is important.

Autoencoders and Anomaly Detection

Autoencoders are effective in unsupervised settings. They are considered adequate for detecting outliers in high-dimensional datasets with scarce labeled data.

C. Advances in Deep Learning

Esenogho et al. (2022) highlight the importance of embedding a neural ensemble model with feature engineering, as this will improve recall and precision. Karthika and Senthilselvi (2023) highlight that dilated convolutional neural networks integrated with sampling techniques are critical in overcoming class imbalance.

D. Challenges and Limitations

Data availability and quality are the first challenges, as these networks require massive labeled datasets for training. These datasets might not always be available. Meanwhile, traditional models perform better with smaller datasets (Alarfaj et al., 2022). Class imbalance is another limitation; fraud cases are rare, mostly less than 1% of the data. Therefore, these models suffer from this limitation. As fraud patterns evolve rapidly, model updating is another challenge, and neural networks can be retrained frequently. However, the process is computationally intensive. It is important to note that traditional systems require manual rule updates. We have adversarial attacks as neural networks are vulnerable to adversarial manipulation. Therefore, fraudsters can exploit model weaknesses, especially in black-box models. Hilal et al. (2022) highlight that despite the success of RNNs, they lack accountability, and this limits their acceptability in regulated financial environments. Albuquerque Filho et al. (2022) emphasizes the need for explainable AI in production-grade anomaly detection.

E. Quantum and Emerging Models

According to Innan et al. (2024), a quantum graph neural network is effective in achieving enhanced fraud detection accuracy. This method can guarantee accuracy with minimal training overhead. It therefore suggests that the future of fraud analytics will likely include quantum and edge-based models.

III. Methodology

The research adopts a comparative analysis framework using secondary data from recent peer-reviewed studies. The fraud detection models were evaluated based on accuracy, interpretability, precision, and recall. They were also evaluated based on adaptability to imbalanced data, scalability, and resource demand. Algorithms that were compared included neural network models, such as CNNs, Ensemble, QGNNs, Graph NNs, DCNN, and RNNs. Traditional models, including SVMs, logistic regression, and decision trees, were also compared. The performance indicators were extracted and compared in structured tables. A hybrid detection architecture is highlighted to demonstrate how different models can be integrated in practice.

IV. Results and Analysis

Table 1: Performance Metrics from Recent Literature

Model	**Accuracy (%)**	**Precision**	**Recall**	**Interpretability**
Logistic Regression	89.0	0.84	0.81	High
Decision Tree	90.7	0.87	0.85	High
Support Vector Machine	91.3	0.89	0.86	Medium
Dilated CNN	96.4	0.92	0.90	Low
Ensemble Neural Network	97.1	0.94	0.95	Low
Quantum GNN	98.2	0.96	0.95	Very Low

V. Proposed Hybrid Architecture

We propose a hybrid fraud detection pipeline to reconcile the strengths of both approaches.

[Transaction]

↓

[Rule-Based Engine] → [Anomaly Score]

↓

[Neural Network Classifier] → [Fraud Decision]

This architecture enhances performance while ensuring compliance. As depicted in Hilal et al. (2022), integrating a rule-based stage can reduce false positives by 30%.

Accuracy and False Positives

The neural network outperforms traditional models regarding precision and recall, especially with imbalanced datasets. Traditional models, however, offer fewer false positives in well-engineered rule-based systems.

Interpretability

Neural networks are criticized due to their black-box nature. Decision trees and logistic regression provide clear reasoning for each decision. This is an important approach for regulatory compliance.

Computational Efficiency

While traditional models are lightweight and efficient, neural networks require huge computational resources and GPU support.

Real-World Deployment

In many real-world financial systems, hybrid models are effective. These models combine rule-based filters with deep learning models, which have been proven to be effective and reliable.

Conclusion

Traditional algorithms and neural networks have their place in fraud detection. They have an important role to play in fraud detection, and therefore, understanding their strengths and limitations is critical in employing them as required. Traditional models are effective as they offer fast performance and, therefore, can be reliable in handling emergencies. They offer interpretability, which is essential in allowing one to comprehend and ease of deployment; thus, implementation is easy. However, traditional models lack adaptability, which limits their use. Neural networks provide higher accuracy and, therefore, reliability. They offer better detection of subtle fraud patterns. They, however, require large datasets and computational resources, and this can limit small players. The future of fraud detection lies in hybrid systems. These systems are effective as they leverage the strengths of both approaches. This is important for robust adaptive systems, as they can guarantee explainable fraud detection frameworks. Companies should ass their specific needs. They must meet regulatory requirements, response time, and dataset size to design or select the most effective system. It is, therefore, important to implement a hybrid model as this will guarantee better fraud detection.

REFERENCES

1. Alarfaj, F. K., Malik, I., Khan, H. U., Almusallam, N., Ramzan, M., & Ahmed, M. (2022). Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms. *Ieee Access*, *10*, 39700-39715. https://ieeexplore.ieee.org/abstract/document/9755930

2. De Albuquerque Filho, J. E., Brandao, L. C., Fernandes, B. J. T., & Maciel, A. M. (2022). A review of neural networks for anomaly detection. *IEEE Access*, *10*, 112342-112367. https://ieeexplore.ieee.org/abstract/document/9925159

3. Esenogho, E., Mienye, I. D., Swart, T. G., Aruleba, K., & Obaido, G. (2022). A neural network ensemble with feature engineering for improved credit card fraud detection. *IEEE access*, *10*, 16400-16407. https://ieeexplore.ieee.org/abstract/document/9698195

4. 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. https://www.sciencedirect.com/science/article/pii/S0957417421017164

5. Innan, N., Sawaika, A., Dhor, A., Dutta, S., Thota, S., Gokal, H., ... & Bennai, M. (2024). Financial fraud detection using quantum graph neural networks. *Quantum Machine Intelligence*, *6*(1), 7. https://link.springer.com/article/10.1007/s42484-024-00143-6

6. Karthika, J., & Senthilselvi, A. (2023). Smart credit card fraud detection system based on dilated

convolutional neural network with sampling technique. *Multimedia Tools and Applications*, *82*(20), 31691-31708. https://link.springer.com/article/10.1007/s11042-023-15730-1

7. Mururunkwere, B. F., Tuyishimire, O., Haughton, D., & Nzabanita, J. (2022). Fraud detection using neural networks: A case study of income tax. *Future Internet*, *14*(6), 168. https://www.mdpi.com/1999-5903/14/6/168

8. Osegi, E. N., & Jumbo, E. F. (2021). Comparative analysis of credit card fraud detection in simulated annealing trained artificial neural network and hierarchical temporal memory. *Machine Learning with Applications*, *6*, 100080. https://www.sciencedirect.com/science/article/pii/S2666827021000402?__cf_chl_rt_tk=0rS2DPjV1RGF8wnckHQSxq2ujfxWkVgi7Y2FTxZlYAw-1751346888-1.0.1.1-oTafKdFjXFZ46z4tneVa4EB11CrSqC7x1SffuTXwzJM

9. Okur, M. R., Zengin-Karaibrahimoglu, Y., & Taşkın, D. (2021). From Conventional Methods to Contemporary Neural Network Approaches: Financial Fraud Detection. *Ethics and Sustainability in Accounting and Finance, Volume III*, 215-228. https://link.springer.com/chapter/10.1007/978-981-33-6636-7_11