International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

Advances In Neural Network for Credit Card Fraud Detection

Aditya Singh[1], Sakshi Srivastava[2]

[1, 2]B. Tech, School Of Computer Science And Engineering
Galgotias University, Gautam Buddha Nagar, UP, INDIA

Abstract
Credit card fraud is the most serious form of risk to financial security and it has a far-reaching effect on consumers and users in general; this makes it necessary that modern methods for machine learning like neural networks should be employed in order to improve their capacity and accuracy for detecting frauds. Various popular neural network architectures for fraud detection, including Feedforward Neural Networks, Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short-Term Memory Networks (LSTM), Autoencoders, and Generative Adversarial Networks (GAN) are investigated in this study.

Keyword: Feedforward Neural Networks (FNN), Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short-Term Memory Networks (LSTM), Autoencoders, Generative Adversarial Networks (GAN)

1. Introduction

A credit card fraud can hugely impact on financial security since it is one of its worst forms; this has an extensive effect on the buyers as well as users at large. With continuous increase in digital transactions, also fraudulent activities have risen. It has become more complex thereby posing a great challenge to fraud detection systems. Conventionally, fraud detection involves use of rule-based systems and statistical methods but they cannot explain the intricacies that come with current day which are different from what they were based on in the past years' transaction systems. This makes it necessary to use advanced machine learning techniques such as neural networks so as to improve ability and precision when detecting frauds [1].

Typically, the detection of fraud relies greatly on systems developed through rules. In some circumstances they use various statistical methods. A number of rule-based systems are designed around finding suspicious transactions using some predefined rules. For instance, alerts that are raised when a transaction has gone beyond a specific amount or where it was made deviates from the norm can be classified as such. Although these types may be adept at detecting known patterns of fraud, they often have difficulty dealing with new or subtle cases since they do not possess any predetermined guidelines.

In addition, statistical approaches for identifying fraudulent transactions via anomaly detection together with clustering have been applied. The latter identify outliers in historical information relative to standard behavior patterns over time. However, these methods capture already existing forms while

ignoring new types of frauds altogether [2]. At the same time rule-based and statistical solutions face the challenge of having high-dimensional and unbalanced datasets where we have very few cases of fraud compared to the total transacted amount.

1.1 Objectives and Scope

The primary objective of the review paper is:

- Examine Neural Network Architectures: Review various neural network models like FNNs, CNNs, RNNs, LSTMs, Autoencoders, and GANs used for detecting credit card fraud.
- Evaluate Transaction Identification: Assess how these neural networks aid in identifying fraudulent transactions and their ability to outperform traditional methods.
- Analyse Performance Metrics: Investigate metrics like precision, recall, F1-score, and AUC-ROC to determine the effectiveness of neural networks in fraud detection.
- Address Major Difficulties: Highlight challenges such as data imbalance, interpretability issues, real-time processing, and computational demands in using neural networks.
- Propose Future Research Directions: Suggest avenues for improving fraud detection models, including new architectures and solutions to current limitations.

2. Background and Traditional Approaches

2.1 Credit Card Fraud Detection Challenges

Financial institutions have made credit card fraud detection one of their biggest challenges due to its major financial and reputation threats. It is complicated by the largest and non-linear transactional data that doesn't change with time and the ever-changing approaches deployed by criminals in perpetrating this crime. By utilizing complex means of imitating the original actions undertaken through credit cards by customers, these fraudsters make it hard to apply simple rules to discriminate between genuine and counterfeit activities.

The main problem lies in the scarcity of fraud occurrences when compared to that of genuine transactions resulting in biasness towards the latter in the development of automated systems for detecting frauds which leads these systems missing frauds detection. This plays a vital role in enhancing effectiveness on fraud detection in such systems.

By evolving their strategies in covering their operations, fraud detection systems must undergo fast changes since new approaches are always being discovered by culprits. Therefore, traditional methods base on past events or static regulations would not be able to adapt with such dynamicity [3].

Therefore, time-dependent models are needed for fraud detection systems so that fraudulent transactions do not serve a clearing house for immediate money transaction execution. However, accuracy remains key to these models yet efficiency conflicts with transaction processing speed requirements.

2.2 Traditional Methods

Rule-Based Systems

Fraud detection using automation system detects potentially fraudulent transactions and refer them. Once fraudsters adjust their methods, it becomes difficult to pursue them because existing processes lack

adaptability.

These systems offer a wealth of information regarding contemporary methodologies; however, they do not have any theoretical framework that may help elucidate rule-based frameworks. It indicates that such frameworks do not exist and are heavily reliant on types of data. Because of its ambiguous nature, numerous swindlers work within this field [4].

2.3 Statistical Models

Historical transaction data is used to discover fraud tendencies using logistic regression and decision trees. Transactions are either fraudulent or real. The models then separate the two categories by transaction amount, merchant type, and location [5].

Statistical models may combine more information and utilize bigger datasets. They are additionally limited by unbalanced fraud and actual transaction predictors that influence forecasts. Complex input variable interactions may cause these statistical models to fail, decreasing their ability to identify sophisticated fraud schemes.

2.4 Machine Learning Algorithms

Fraud detection has improved using machine learning methods like Random Forests and Gradient Boosting Machines. Ensemble approaches combine several dependable models to generate one final prediction, improving accuracy and reliability above typical statistical models [6].

Random Forest uses numerous decision trees on categorized transactions and consolidates their results to make a judgment. This stabilizes data variance and minimizes overfitting. Gradient Boosting Machines repeatedly correct model faults. This makes classifying all transactions more difficult, but the model becomes more predictable.

Machine learning algorithms have similar difficulties as previous approaches. They may overfit if not monitored and require adjusted hyperparameters. Their results may not reflect their decision-making rules.

2.5 Anomaly Detection Techniques

Any transaction anomaly detection method seeks to identify abnormal transactions. The most common methods assume that there are few frauds in a sample and that they vary considerably from genuine transactions. Clustering and distance-based methods are examples [7].

Outliers are transactions that do not belong to any cluster, whereas K-means cluster comparable transactions [8]. Another example is distance-based algorithms like KNN that identify suspicious transactions with large gaps between them.

Anomaly detection methods assist find new or unexpected fraudulent trends; however, their notion of normalcy might be quite imprecise, resulting in numerous false positives.

2.6 Hybrid Approaches

Hybrid techniques overcome limits by combining different methods' strengths. Hybrid systems may filter transactions using rules before using machine learning techniques. A balance must be struck between processing speed and detecting increasingly complicated fraud behaviors.

Thus, hybrid techniques should improve detection accuracy and minimize false positives by using several data sources and models [9].

Well-established transaction fraud detection methods including rule-based, statistical, and machine learning algorithms do not sufficiently depict the dynamic nature of fraud and lack of resilience in one-directional transaction data. Several anomaly detection methods struggle to define typical behavior. As fraud strategies evolve, more complex solutions to tackle such challenges are needed.

Neural networks can model complicated patterns and learn from huge data, making them the best credit card fraud detection option. This section discusses how neural networks overcome existing approaches' limitations and offers new fraud detection potential [10].

3. Neural Network Architectures for Fraud Detection

Neural networks have been shown to be exceptionally useful in credit card fraud detection. This is primarily because of their capabilities in capturing complex correlations and dependencies between transaction variables. Different types of neural network models have been tested and used for better fraud detection systems. In this module, we discuss some of the commonly used neural network architectures utilized in fraud detection – Feedforward Neural Networks, Convolutional Neural Networks, Recurrent Neural Networks, Long Short-Term Memory Networks, Autoencoder and Generative Adversarial Networks.

3.1 Feedforward Neural Networks (FNNs)

FNNs are the simplest neural network. They have hidden, input, and output layers. FNNs identify credit card fraud by finding complex relationships between transaction variables and fraud risk [11].

Simple data flow characterizes FNN architecture. Since this network cannot reverse output to input, information flows only one direction. FNNs link first- and second-layer neurons. Connectivity helps analyze complicated transaction data relationships.

FNNs readily identify non-linear transaction attribute-fraud flag relationships. Inconsistent spending or transaction quantities may suggest fraud. FNNs may imitate complex fraud patterns.
Despite their simplicity and ease of creation, FNNs have issues. Transactional data seldom provide sequential dependence for over-time pattern retrieval. FNNs require rigorous preprocessing and selection of the most relevant features to operate well, and they cannot automatically assess variable significance without pre-training.

3.2 Convolutional Neural Networks (CNNs)

They process images efficiently, thus they're popular. Sequences or geographical layouts of transaction data may help indicate credit card fraud. CNNs examine pixels but arrange data.

CNN convolutional layers automatically extract crucial data characteristics. By finding patterns in incoming data, convolutional filters reveal essential characteristics and spatial connections. Pooling layers minimize dimensionality while keeping peak feature extraction following convolutional layers. Hierarchical patterns connect key data variables throughout this process.

CNNs can detect fraud by visualizing transaction data as a geographical grid. It has shown hierarchical structures and geographical linkages that may suggest fraud. Thus, this CNN may discover intricate transaction-hidden pattern correlations that earlier methods cannot.

CNN fraud detection is limited. This method works well with geographical data but badly with sequential or temporal data if not stated. Tuning convolution filters and pooling algorithms to optimize CNN performance is complicated since it requires a better grasp of the data and the job at hand to discover crucial fraud features [12].

3.3 Recurrent Neural Networks (RNNs)

RNNs accept sequential input and feedback preceding time steps at every output level. Time-series and transaction analysis benefit from RNNs' temporal linkages. RNNs identify credit card fraud better over time. Due to level feedback loops, RNNs may store transaction data. Thus, RNNs may "remind" themselves of previous inputs to model transaction linkages and detect fraud. A user's incremental spending patterns over several transactions may be fraud anomalies to RNNs.

RNNs aid long-term fraud since they are not isolated. From breaches in an individual's usual purchase history, RNNs may discover sequence-based anomalous buying behaviors. RNNs detect low-intensity frauds missed by conventional models by analyzing transaction sequences.
Traditional RNNs are flawed. Gradients disappearing and increasing make long-term dependencies hard for the network to grasp. Network gradients drop or grow too much during training, affecting long-range correlation learning. RNNs may use LSTM networks or GRUs to detect temporal trends across long transaction strings [13].

3.4 Long Short-Term Memory (LSTM) Networks

Long short-term memory networks improve RNN shortcomings. LSTMs ensure long-term consistency when transferring memory cell information.
Input, output, and forget gates govern LSTM memory cell input and output. The forget gate controls loss, the input gate controls data entering the memory cell, and the output gate controls output. Thus, crucial information may be remembered while minor details lost. LSTMs memorize and utilize prior step data better than RNNs. They aid long-term pattern comprehension.
LSTMs identify credit card fraud because transaction analysis uses sequential data with long-term trends and dependencies. Over time or transactions, LSTMs may indicate fraudulent spending. Due to its long-term reliance, LSTMs may detect small transaction pattern changes that may suggest fraud [14].

LSTMs have drawbacks despite outperforming RNNs. They demand huge RAMs for storing and more computation for training and tuning than RNNs. LSTM's complex architecture requires thorough hyperparameter tuning for best performance. LSTMs handle delayed relationships better than RNNs, although prolonged sequences hinder model processing. The network topology, processing power, and when to deploy LSTM against fraud are crucial.

3.5 Autoencoders

Unsupervised learning heavily leverages neural networks. Their major purpose is compressed input data representation learning. Anomaly detection technology can reproduce data that departs from regular behavior, aiding credit card fraud detection. An autoencoder compresses input data into a lower-dimensional latent space, while the decoder reconstructs it. Model representation of its training set is measured by reconstruction error.

This makes autoencoders valuable for fraud detection. Transaction data with substantial reconstruction errors from this anomaly detection method are likely fake since they deviate from learnt transaction patterns. Thus, autoencoders may spot transactions that deviate from the model's spending trend.

Notably, autoencoders have restrictions. They employ large datasets to analyze and manage information and are impacted by brain shape and learning rate. More importantly, autoencoders' fraud detection is confined to estimates since they use average transactions. In frequent and changing fraud situations, this reduces the tool's efficiency and usefulness.

3.6 Generative Adversarial Networks (GANs)

Generative Adversarial Networks is a neural network architectural framework containing two conflicting networks: the discriminator, which separates actual samples from generator-generated ones, and the generator, which seeks to approximate originals. Over time, fake data improves and patterns become apparent [15].

Fraud detection benefits from GAN architecture. An illicit transaction may be generated and validated by a discriminator. Both networks benefit from this adversarial process: the generator improves at replicating fraudulent patterns while the discriminator improves at identifying actual transactions. This partnership creates high-quality fraud-detection training algorithm imitation examples.
GANs aid data imbalance applications. Compared to genuine transactions, fraud is infrequent. GANs redistribute data for machine learning model training using phony fraud examples. Learning from adverse situations is another GAN advantage. They may identify new or concealed fraud trends, which may help them develop new fraud methods.

TABLE 1. Names of the Architectures

Architecture	Key Points
FNNs	Simple, detects non-linear patterns, but lacks temporal processing and requires preprocessing.
CNNs	Effective for spatial data, but

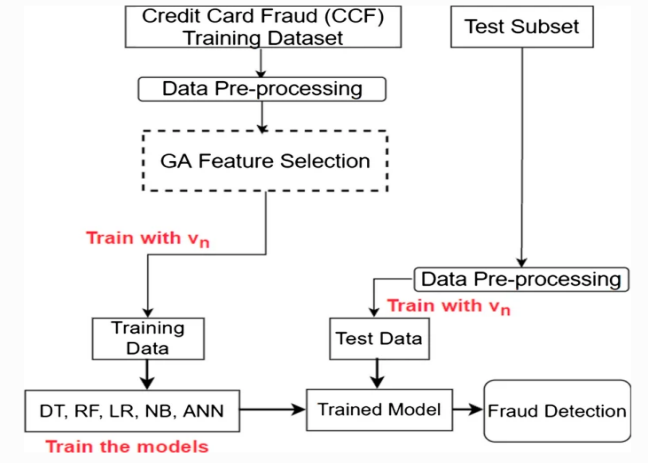
	struggles with sequential data and requires optimization
RNNs	Captures temporal patterns, but has issues with long-term dependencies.
LSTMs	Better for long-term dependencies, but computationally expensive.
Autoencoder	Detects anomalies without labeled data, but needs large datasets and struggles with evolving fraud.
GANs	Generates synthetic fraud data, but requires significant computational resources.

Source: "Deep Learning" by Ian Goodfellow, Yoshua Bengio, and Aaron Courville

4. Evaluation Metrics and Performance

Models of machine learning must undergo critical evaluation for the proper assistance of credit card fraud detection in such a way that fraudulent transactions are correctly identified while minimizing false positives. In these datasets, the nature is highly imbalanced where frauds may only constitute a tiny percentage of the whole data set. Therefore, in this situation, accuracy alone cannot be seen as performance measure since it often poorly represents fraudulent transactions and tend to be biased. Instead, more often helpful for detection tasks are metrics oriented to the minority-classed victims such as precision, recall, F1-score or area under the Receiver Operating Characteristic (ROC) curve.

Fig. 1



Architecture of the proposed framework.

5. Accuracy

In evaluating machine learning models, accuracy is one of the most commonly used metrics that show how many instances were predicted correctly as either fraud or non-fraud out of total predictions. For instance, one can tell how the model is performing basing on this metric but in fraud detection, it is generally speaking a very misleading metric. This is due to the fact that fraudulent transactions occur

rarely so even if this model predicts all transfers as if they are not fraudulent, it might still be accurate because numerous legit transactions take place most of the time. On the other hand, such a model will not catch frauds and accuracy itself becomes less important in strongly imbalanced datasets.

6. Precision and Recall

The most common fraud detection model assessment criteria are recall and accuracy. These tests illustrate how effectively the model recognizes minority class or fraud.

Truly positive fraud transactions make up precision over all positive fraud predictions. It seeks predictive accuracy. High accuracy decreases false positives and alarms.

Recall evaluates software fraud detection. Recall true positives for well and poorly classified fraud. If recall scores are high, most fraudulent transactions were discovered, although incorrectly.

Detecting fraud requires precision above memory. High recall models may flag more suspicious transactions as fraudulent, resulting in more false positives, whereas high precision models may be excessively cautious to avoid false positives. Application-specific precision and recall may be swapped. If avoiding false positives is more essential than uncovering all frauds, retrieval rates will be lower, but if detecting as many as possible is needed, there must be a margin for error.

7. F1 Score

F1-score, based on accuracy and recall, is a reliable model assessment. It is the harmonic mean of accuracy and recall. The equation accounts for precision-recall tradeoffs. F1-score is ideal for fraud detection since perfect accuracy and recall are hard to acquire.

Fraud detection will improve with greater F1. As with accuracy and recall, the F1-score depends on whether fraud judgments are taken at the transaction level. Thus, fine-tuning threshold values is crucial to optimizing F1 scores for fraud detection systems.

8. ROC and AUC

The ROC curve is the most significant fraud detection model evaluation tool. For many threshold levels, the ROC curve shows the true positive rate, or recall, on the Y-axis and the false positive rate on the X-axis. A strong fraud detection model has a ROC curve that approaches the top-left corner of the plot with high true positives and low false positives.

As a scalar summary of all model thresholds, AUC-ROC is commonly presented. Random guessing is 0.5, optimum to 1.0 so the model can distinguish fraudulent from authentic transactions.

9. Confusion Matrix

A classification model can be presented through confusion matrix which derives true positive, true negatives, false positive and false negatives. Considering fraud detection in more particulars, we have:

- True Positives (TP) refer to True Fraudulent Transactions that are correctly identified;
- True Negatives: They are rightly labelled legitimate transactions;

- False Positives (FP) or Type I errors: These represent actual transactions that have been misclassified as fraudulent;
- False Positives/FN (Type II errors): These encompass those fraudulent transactions that passed without being noticed and consequently considered as legal ones.

It is through the confusion matrix that model's training errors type's presence during training as well as an accurate indication of its performance understanding is given.

10. Future Direction and Conclusion

Credit card fraud trends fluctuate, making detection accuracy and consumer satisfaction a constant struggle. Credit card fraud detection has uneven class distribution. Because real transactions dominate fake ones. However, credit card fraud techniques change, making detection vital. Therefore, fraud detection systems require reinforcement learning or continuous learning models that adapt fast.

Another problem is class disparity. Fraudulent transactions are rare in most fraud detection databases. This typically means the algorithm learns to predict more non-frauds and is accurate but inaccurate on genuine frauds. Overfitting is difficult to prevent, however oversampling using SMOTE or GANs may address this imbalance.

Security and privacy of data are crucial. Transaction history, personal information, and payment methods are used in several fraud detection approaches. Protecting data from unauthorized contact while letting the model learn is difficult. Differentiate privacy and federated learning, which let models learn from decentralized data while preserving personal data, are currently being developed.

Future research will emphasize explain ability. Many fraud detection systems, particularly deep learning ones, are "black boxes"—hard to grasp. Transparency issues would make companies mistrust this technology, hurting customers. Build confidence in these platforms via interpretable models or explain ability methods like SHAP or LIME.

Financial institutions execute millions of transactions every day, so fraud detection technologies must be accurate and scalable. Faster algorithms or distributed computing may help.

Complex and dynamic credit card fraud detection. Classic models can't handle dynamic fraud, class imbalance, and privacy issues; hence they can't use neural networks. CNNs, RNNs, LSTMs, and GANs increase detection, but they are costly, complicated, and need careful tuning.

Data privacy and model transparency might increase with adaptive models, creating scalable and effective fraud smart detection systems. To stay ahead of payment card simulator-using fraudsters, future fraud detection systems will include the newest fraudster strategies.

REFERENCES

[1] Rb, A., & Kr, S. K. (2021). Credit card fraud detection using artificial neural network. *Global Transitions Proceedings*, *2*(1), 35–41. https://doi.org/10.1016/j.gltp.2021.01.006

[2] *Credit Card Fraud Detection using Artificial Neural Network and BackPropagation*. (n.d.). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/9120957
[3] Georgieva, S., Markova, M., & Pavlov, V. (2019). Using neural network for credit card fraud detection. *AIP Conference Proceedings*. https://doi.org/10.1063/1.5127478
[4] *A Dual Approach for Credit Card Fraud Detection using Neural Network and Data Mining Techniques*. (n.d.). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/9342462
[5] Ghosh, S., & Reilly, D. L. (1994). *Credit card fraud detection with a neural-network*. https://www.semanticscholar.org/paper/Credit-card-fraud-detection-with-a-neural-network-Ghosh-Reilly/ba70a74262adec9dcfa47b5710752d2537a07af4
[6] Pillai, T. R., Hashem, I. a. T., Brohi, S. N., Kaur, S., & Marjani, M. (2018). Credit Card Fraud Detection Using Deep Learning Technique. *ICACCA*. https://doi.org/10.1109/icaccaf.2018.8776797
[7] Sulaiman, S. S., Nadher, I., & Hameed, S. M. (2024). Credit card fraud detection using improved deep learning models. *Computers, Materials & Continua/Computers, Materials & Continua (Print)*, *78*(1), 1049–1069. https://doi.org/10.32604/cmc.2023.046051
[8] Karthikeyan, T., Govindarajan, M., & Vijayakumar, V. (2023). An effective fraud detection using competitive swarm optimization based deep neural network. *Measurement Sensors*, *27*, 100793. https://doi.org/10.1016/j.measen.2023.100793
[9] Zou, J., Zhang, J., & Jiang, P. (2019, August 30). *Credit card fraud detection using autoencoder neural network*. arXiv.org. https://arxiv.org/abs/1908.11553
[10] Marie-Sainte, S. L., Alamir, M. B., Alsaleh, D., Albakri, G., & Zouhair, J. (2020). Enhancing credit card fraud detection using deep neural network. In *Advances in intelligent systems and computing* (pp. 301–313). https://doi.org/10.1007/978-3-030-52246-9_21
[11] Gulati, A., Dubey, P., MdFuzail, C., Norman, J., & Mangayarkarasi, R. (2017). Credit card fraud detection using neural network and geolocation. *IOP Conference Series Materials Science and Engineering*, *263*, 042039. https://doi.org/10.1088/1757-899x/263/4/042039
[12] Fu, K., Cheng, D., Tu, Y., & Zhang, L. (2016). Credit card fraud detection using convolutional neural networks. In *Lecture notes in computer science* (pp. 483–490). https://doi.org/10.1007/978-3-319-46675-0_53
[13] *The International Arab Journal of Information Technology*. (n.d.). https://www.iajit.org/paper/1959/Credit-card-Fraud-Detection-System-using-Neural-Networks
[14] Sadgali, I., Sael, N., & Benabbou, F. (2019). Fraud detection in credit card transaction using neural networks. *Proceedings of the 4th International Conference on Smart City Applications*. https://doi.org/10.1145/3368756.3369082
[15] Benchaji, I., Douzi, S., Ouahidi, B. E., & Jaafari, J. (2021). Enhanced credit card fraud detection based on attention mechanism and LSTM deep model. *Journal of Big Data*, *8(*1). https://doi.org/10.1186/s40537-021-00541-8
[16] Ileberi, E., Sun, Y. & Wang, Z. A machine learning based credit card fraud detection using the GA algorithm for feature selection. *J Big Data* **9**, 24 (2022). https://doi.org/10.1186/s40537-022-00573-8