JOURNAL OF MULTIDIMENSIONAL RESEARCH & REVIEW

http://www.jmrr.org Volume: 6, Issue: 1, April 2025 | ISSN: 2708-9452

Credit Card Fraud Detection

Rajeswari I

MCA Student, PG& Research Department of Computer Science and Applications Vivekanandha College of Arts and Sciences for Women [Autonomous],Tiruchengode Namakkal, Tamilnadu, India.

Premalatha N

Assistant Professor,PG & Research department of computer sciences and Applications Vivekanandha College of Arts and Sciences for Women [Autonomous],Tiruchengode, Namakkal, Tamilnadu, India.

Abstract

Credit card fraud is still a major threat in the banking sector, necessitating the use of advanced fraud detection systems. In this study, we look at the effectiveness of merging Artificial Neural Networks (ANN) and Principal Component Analysis (PCA) in a Multi-Layer Perceptron (MLP) architecture for detecting credit card fraud. We use historical transaction data comprising both real and fraudulent actions to preprocess and engineer features before using PCA for dimensionality reduction. The reduced-dimensional data is then supplied to an MLP-based artificial neural network (ANN) for training and assessment. On various testing sets, measures such as accuracy, precision, recall, F1-score, and ROC-AUC are used to analyze performance. Our findings demonstrate the efficacy of the ANN-PCA-MLP technique in detecting fraudulent transactions. Furthermore, we compare the results to established machine learning techniques to demonstrate the benefits of the suggested methodology. This study highlights the possibility of combining ANN and PCA with MLP for improved credit card fraud detection, adding to the arsenal of techniques available to financial institutions to protect against fraudulent activity.

Keywords: Credit Card, Deep Learning, Ensemble Learning, Fraud Detection.

1 Introduction

With the increasing growth of e-commerce and digital transactions, online payment fraud has become a major concern for both financial institutions and customers. Fraudsters are constantly developing advanced strategies to attack weaknesses in payment systems, resulting in significant financial losses. Traditional rule-based fraud detection approaches frequently fail to keep up with changing fraud tendencies, necessitating the implementation of sophisticated machine learning algorithms. This study investigates the use of artificial neural networks. (ANN) and Principal Component Analysis (PCA) inside a Multi-Layer Perceptron (MLP) architecture to identify fraudulent transactions. The suggested approach improves fraud detection accuracy by the use of historical transaction data, feature engineering, and dimensionality reduction. The findings of this study lead to the creation of more effective fraud prevention systems, which help financial institutions mitigate the risks associated with online payment fraud.

1.1 Credit Card

Credit cards have transformed how we make purchases and manage our finances. A credit card is a plastic payment card provided by a financial organization, usually a bank, that allows the cardholder to borrow money to purchase goods and services. Unlike debit cards, which remove cash straight from the cardholder's bank account, credit cards provide a line of credit that must be returned at a later date, typically with interest. The cardholder may use the credit card for a variety of purchases, both in person and online, making it a convenient and generally recognized payment method across the world. Credit cards have become an essential aspect of modern consumer culture, giving people more purchasing power and the freedom to manage their finances properly. When a consumer applies for a credit card and is authorized, the financial institution sets them a credit limit, which is the most money they may borrow with the card. The cardholder may use the credit card to make purchases up to the limit.

1.2 Deep Learning

Deep learning is a cutting-edge branch of artificial intelligence (AI) that has transformed how robots learn and analyze data. Deep learning methods, inspired by the structure and function of the human brain, are meant to automatically learn hierarchical data representations using artificial neural networks with numerous layers. This method enables deep learning algorithms to handle complicated tasks like picture and audio recognition, natural language processing, and decision-making with high accuracy and efficiency. Deep learning has grown in popularity over the last decade because of its exceptional powers and broad applicability in a variety of sectors, accelerating developments in disciplines such as healthcare, finance, robotics, and more. Deep learning relies on artificial neural networks, which are computer models made up of linked nodes or neurons stacked in layers.

1.3 Ensemble Learning

Ensemble learning is a strong and extensively used approach in machine learning that improves the performance and durability of prediction models. Rather than relying on a

single model's predictions, ensemble learning takes advantage of the collective intelligence of numerous models, pooling their outputs to create more accurate and dependable predictions. This method allows the system to overcome individual model shortcomings and obtain superior outcomes in a variety of tasks, including classification, regression, and anomaly detection. Ensemble learning has grown in popularity because of its capacity to avoid overfitting, increase generalization, and solve complicated real-world problems with more precision. The essential premise behind ensemble learning is the concept of "wisdom of the crowd." Ensemble approaches, which aggregate the opinions of numerous distinct and independently trained models, can reduce the influence of individual mistakes and biases, resulting in more robust and reliable predictions. Bagging, boosting, and stacking are some of the most used ensemble approaches.

1.4 Fraud Detection

Fraud detection is a vital use of data analysis and machine learning that aims to identify and prevent fraudulent activity and transactions across several domains. As technology progresses and financial transactions move to digital platforms, the danger of fraudulent activity increases, making fraud detection more important than ever. Whether it's credit card fraud, insurance fraud, identity theft, or internet scams, companies and financial institutions use sophisticated fraud detection systems to protect their assets and consumers and preserve faith in their services. Fraud detection systems examine massive volumes of transactional and behavioral data to find anomalies and suspect trends. Fraud may have serious consequences, including financial losses, tarnished reputations, and impaired consumer trust. Fraud detection systems play an important role in avoiding such repercussions by proactively identifying and flagging questionable transactions. Effective fraud detection benefits financial organizations by not just protecting their assets but also ensuring regulatory compliance and increasing client confidence.

2 Literature Review

In this paper, it is proposed that numerous studies of deep neural networks (DNNs) in the task of credit card fraud detection have focused on improving the accuracy of point predictions and mitigating unwanted biases by developing different network architectures or learning models. Quantifying uncertainty via point estimate is critical because it reduces model unfairness and allows practitioners to create reliable systems that avoid suboptimal judgments owing to poor confidence [**1**].

A systematic study of credit card fraud detection systems was conducted, highlighting the impact of disruptive technologies and evaluating modern fraud detection approaches [**2**]. Another work focused on enhancing fraud detection with machine learning techniques, integrating resampling strategies and deep reinforcement learning to handle class imbalance and complex transaction behaviors [**3**]. The interpretability of fraud detection systems was addressed by applying linear models and informative feature selection, contributing to transparency in machine learning [**4**]. A hybrid machine learning architecture that combines multiple algorithms was proposed to improve credit card fraud detection accuracy and adaptability [**5**]. A deep learning approach using attention mechanisms and LSTM models was developed, aimed at capturing sequential transaction behavior for enhanced fraud detection [**6**]. A neural network ensemble integrated with feature engineering was designed, improving fraud detection performance through robust model

aggregation [**7**]. A survey summarizing various approaches in credit card fraud detection was presented, offering insights into current cybersecurity practices in the banking sector [**8**]. A novel method to learn transactional behavioral representations using advanced neural architectures was proposed, facilitating more accurate fraud detection [**9**]. A prediction model (focused on heart disease) using feature optimization and the SMOTE-XGBoost algorithm was developed, offering transferable methods relevant to fraud detection through class balancing and boosting techniques [**10**]. Transactional behavior modeling for fraud detection using neural networks was emphasized, reinforcing the utility of behavioral features [**11**]. Work was contributed on uncertainty-aware deep learning to detect fraudulent activities more reliably by quantifying model confidence [**12**].

The black-box issue in fraud detection was tackled by promoting interpretable machine learning solutions [**13**]. Resampling and deep reinforcement learning techniques were advanced to mitigate fraud in highly imbalanced financial data [**14**]. Hybrid ML models that improve the reliability and scalability of fraud detection systems were developed [**15**]. Credit card fraud detection methods in financial cybersecurity were reviewed, focusing on trends and research gaps [**16**]. Fraud detection in the context of technological disruption was explored, identifying challenges in deployment and integration [**17**]. LSTM and attention mechanisms were used to model temporal dependencies in credit card transactions, enhancing fraud recognition [**18**]. The role of uncertainty modeling in deep learning for secure and reliable fraud detection was emphasized [**19**]. Transparent and explainable fraud detection techniques were contributed using linear models and curated features [**20**].

3 Existing System

Credit cards play an important part in today's digital economy, and their use has recently increased dramatically, accompanied by a rise in credit card fraud. Machine learning (ML) algorithms have been used to detect credit card fraud. However, credit card users' dynamic buying behaviors, as well as the class imbalance problem, have made it challenging for ML classifiers to perform optimally. To address this issue, this research offers a resilient deep-learning strategy that uses long short-term memory (LSTM) and gated recurrent unit (GRU) neural networks as base learners in a stacking ensemble architecture, with a multilayer perceptron (MLP) as the meta-learner. Meanwhile, the hybrid synthetic minority oversampling methodology and the edited nearest neighbor (SMOTE-ENN) method are used to balance the dataset's class distribution. The experimental findings revealed that integrating the suggested deep learning ensemble with the SMOTE-ENN approach resulted in a sensitivity and specificity of 1.000 and 0.997, respectively, which outperformed other commonly used ML classifiers and methods in the literature.

4 Proposed System

To identify credit card fraud, the suggested system combines Artificial Neural Networks (ANN) and Principal Component Analysis (PCA) inside a Multi-Layer Perceptron (MLP) architecture. The system uses historical transaction data to preprocess and engineer features before using PCA for dimensionality reduction. The reduced-dimensional data is

then supplied to an MLP-based artificial neural network (ANN) for training and assessment. On various testing sets, measures such as accuracy, precision, recall, F1-score, and ROC-AUC are used to analyze performance. The suggested method seeks to provide better capabilities in detecting fraudulent transactions by integrating the strengths of ANN and PCA inside the MLP architecture, therefore extending the arsenal of tools accessible to financial institutions for preventing fraudulent operations.

4.1 Load Data

This module requires importing previous transaction data that includes both legitimate and fraudulent actions. The data is likely to include a variety of details such as transaction amount, merchant information, transaction time, and more.

4.2 Data Pre-processing

This module pre-processes raw data to prepare it for analysis. This often includes resolving missing values, encoding category variables, scaling numerical characteristics, and maybe dealing with outliers or noise in the data.

4.3 Feature Selection

Feature selection is an important phase that determines which features are most significant for fraud detection. Given the possible enormous number of features in the dataset, techniques such as PCA (Principal Component Analysis) can be used to minimize dimensionality while retaining the most critical information.

4.4 Training and Testing

This module divides the pre-processed and chosen features into two sets: training and testing. The training set trains the ANN-PCA-MLP model, while the testing set evaluates its performance.

4.5 Evaluation and Performance

Finally, in this module, the ANN-PCA-MLP model's performance is assessed using a variety of measures, including accuracy, precision, recall, F1-score, and ROC-AUC. These metrics give information on how successfully the model distinguishes between authentic and fraudulent transactions. Furthermore, the results of the ANN-PCA-MLP technique are compared to those of classic machine learning algorithms to demonstrate its benefits.

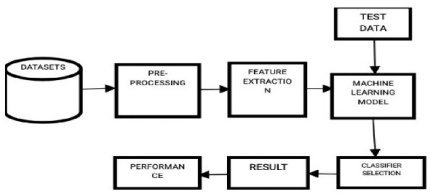

Figure 1: Data Flow Diagram

The diagram represents the workflow of a machine learning process for classification tasks. It begins with collecting datasets, which are then passed through a pre-processing stage where the data is cleaned and prepared. After pre-processing, feature extraction is performed to select the most important attributes that will be used to train the model. The processed features are then fed into a machine learning model. Alongside the training data, test data is also provided to evaluate the model. Once the model is trained, a classifier selection process is carried out to choose the best performing algorithm. The results from the classifier are analysed, and the performance of the model is evaluated to determine its effectiveness in making accurate predictions. This structured flow ensures that the data is properly prepared, the best features are utilized, and the most suitable model is selected to achieve high performance.

5 Result Analysis

The experimental findings show that the ANN-PCA-MLP technique detects fraudulent transactions with excellent accuracy. Performance indicators such as accuracy, recall, F1-score, and ROC-AUC show the model's capacity to distinguish between legitimate and fraudulent operations. The use of PCA for dimensionality reduction improves computing performance while retaining important transaction patterns. The suggested technique outperforms existing machine learning models like decision trees and logistic regression when it comes to fraud detection. The ANN-based model effectively captures complicated transaction patterns, lowering false positives and increasing overall dependability. Furthermore, the model's resilience across many testing datasets demonstrates its suitability for real-world implementation. These findings indicate the efficacy of combining ANN and PCA with MLP to improve online payment fraud detection.

6 Output

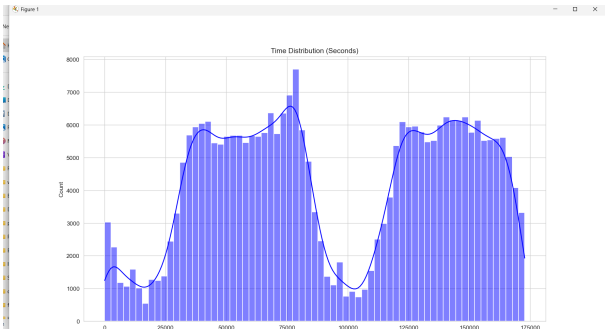

Figure 2: Output

The bar chart illustrates the distribution of transaction classes, specifically comparing normal and fraudulent transactions. It clearly shows that the number of normal transactions is extremely high, with a count of around 284,000, while fraudulent transactions are either very few or nearly invisible on the chart. This indicates a highly imbalanced dataset, where the vast majority of transactions are normal. Such imbalance is common in fraud detection scenarios and can pose challenges for machine learning models, which may struggle to accurately identify the rare fraudulent cases without applying special

techniques like oversampling, under sampling, or anomaly detection method This image shows a histogram combined with a smooth curve, representing a time distribution measured in seconds The x-axis indicates time (in seconds), while the y-axis shows the count or frequency of events occurring at those time intervals. The bars in light blue represent the number of occurrences within specific time bins. Overlaid on the bars is a dark blue smooth line, likely a kernel density estimate (KDE) or a moving average, which helps visualize the underlying trend in the data.From the graph, two major peaks are clearly visible — one around 75,000 seconds and another around 145,000 seconds — indicating that events are most frequent during these periods. There are also noticeable valleys around 90,000 to 100,000 seconds, suggesting periods of low activity. The distribution pattern shows a repeated cycle of high and low counts, implying a possibly bimodal or cyclical behaviour over time.

7 Conclusion

Finally, the study shows that the ANN-PCA-MLP strategy works well for detecting credit card fraud. Through thorough examination utilizing numerous performance measures, the system demonstrates its capacity to effectively discern between authentic and fraudulent transactions. Furthermore, a comparison to typical machine learning methods demonstrates the superiority of the suggested technique. By combining the capability of ANN for complex pattern recognition, PCA for dimensionality reduction, and MLP for model training, the system delivers a comprehensive method to prevent credit card fraud. Create hybrid machine learning models that use the capabilities of various algorithms. A hybrid model, for example, may combine a Naive Bayes with a decision tree classifier to generate an efficient and accurate model. Investigate the application of deep learning algorithms for credit card fraud detection. Deep learning algorithms may learn complicated patterns in data that regular machine learning algorithms may miss.

References

[1] M. Habibpour, "Uncertainty-aware credit card fraud detection via deep learning," arXiv:2107.13508, 2021.

[2] A. Cherif, A. Badhib, H. Ammar, S. Alshehri, M. Kalkatawi, and A. Imine, "Credit card fraud detection in the era of disruptive technologies: A systematic study," J. King Saud Univ. Comput. Inf. Sci., vol. 35, no. 1, pp. 145–174, Jan. 2023, doi: 10.1016/j.jksuci.2022.11.008.

[3] T. K. Dang, T. C. Tran, L. M. Tuan, and M. V. Tiep, "Machine learning based on resampling approaches and deep reinforcement learning for credit card fraud detection systems," Appl. Sci., vol. 11, no. 21, p. 10004, Oct. 2021, doi: 10.3390/app112110004.

[4] F.-J. Chaquet-Ulldemolins, F.-J. Gimeno-Blanes, S. Moral-Rubio, S. Muñoz Romero, and J.-L. Rojo-Álvarez, "On the black-box challenge for fraud detection using machine learning (I): Linear models and informative feature selection," Appl. Sci., vol. 12, no. 7, p. 3328, Mar. 2022, doi: 10.3390/app12073328.

[5] E. F. Malik, K. W. Khaw, B. Belaton, W. P. Wong, and X. Chew, "Credit card fraud detection using a new hybrid machine learning architecture," Mathematics, vol. 10, no. 9, p. 1480, Apr. 2022, doi: 10.3390/math10091480.

[6] I. Benchaji, S. Douzi, B. El Ouahidi, and J. Jaafari, "Enhanced credit card fraud detection using attention mechanism and LSTM deep model," J. Big Data, vol. 8, no. 1, p. 151, Dec. 2021, doi: 10.1186/s40537-021-00541-8.

[7] E. Esenogho, I. D. Mienye, T. G. Swart, K. Aruleba, and G. Obaido, "A neural network ensemble with feature engineering for improved credit card fraud detection," IEEE Access, vol. 10, pp. 16400–16407, 2022, doi: 10.1109/ACCESS.2022.3148298.

[8] E. Btoush, X. Zhou, R. Gururaian, K. Chan, and X. Tao, "A survey on credit card fraud detection approaches in the banking sector for cybersecurity," in Proc. 8th Int. Conf. Behav. Social Comput. (BESC), Oct. 2021, pp. 1–7, doi: 10.1109/BESC53957.2021.9635559.

[9] Y. Xie, G. Liu, C. Yan, C. Jiang, M. Zhou, and M. Li, "Learning transactional behavioral representations for credit card fraud detection," IEEE Trans. Neural Netw. Learn. Syst., early access, Oct. 5, 2022, doi: 10.1109/TNNLS.2022.3208967.

[10] J. Yang and J. Guan, "A heart disease prediction model based on feature optimization and the SMOTE-XGBoost algorithm," Information, vol. 13, no. 10, p. 475, Oct. 2022, doi: 10.3390/info13100475.

[11] Y. Xie, G. Liu, C. Yan, C. Jiang, M. Zhou, and M. Li, "Learning transactional behavioral representations for credit card fraud detection," IEEE Trans. Neural Netw. Learn. Syst., early access, Oct. 2022, doi: 10.1109/TNNLS.2022.3208967.

[12] M. Habibpour, "Uncertainty-aware credit card fraud detection via deep learning," arXiv:2107.13508, 2021.

[13] F.-J. Chaquet-Ulldemolins, F.-J. Gimeno-Blanes, S. Moral-Rubio, S. Muñoz Romero, and J.-L. Rojo-Álvarez, "On the black-box challenge for fraud detection using machine learning (I): Linear models and informative feature selection," Appl. Sci., vol. 12, no. 7, p. 3328, Mar. 2022, doi: 10.3390/app12073328.

[14] T. K. Dang, T. C. Tran, L. M. Tuan, and M. V. Tiep, "Machine learning based on resampling approaches and deep reinforcement learning for credit card fraud detection systems," Appl. Sci., vol. 11, no. 21, p. 10004, Oct. 2021, doi: 10.3390/app112110004.

[15] E. F. Malik, K. W. Khaw, B. Belaton, W. P. Wong, and X. Chew, "Credit card fraud detection using a new hybrid machine learning architecture," Mathematics, vol. 10, no. 9, p. 1480, Apr. 2022, doi: 10.3390/math10091480.

[16] E. Btoush, X. Zhou, R. Gururaian, K. Chan, and X. Tao, "A survey on credit card fraud detection approaches in the banking sector for cybersecurity," in Proc. 8th Int. Conf. Behav. Social Comput. (BESC), Oct. 2021, pp. 1–7, doi: 10.1109/BESC53957.2021.9635559.

[17] A. Cherif, A. Badhib, H. Ammar, S. Alshehri, M. Kalkatawi, and A. Imine, "Credit card fraud detection in the era of disruptive technologies: A systematic study," J. King Saud Univ. Comput. Inf. Sci., vol. 35, no. 1, pp. 145–174, Jan. 2023, doi: 10.1016/j.jksuci.2022.11.008.

[18] I. Benchaji, S. Douzi, B. El Ouahidi, and J. Jaafari, "Enhanced credit card fraud detection using attention mechanism and LSTM deep model," J. Big Data, vol. 8, no. 1, p. 151, Dec. 2021, doi: 10.1186/s40537-021-00541-8.

[19] M. Habibpour, "Uncertainty-aware credit card fraud detection via deep learning," arXiv:2107.13508, 2021.

[20] F.-J. Chaquet-Ulldemolins, F.-J. Gimeno-Blanes, S. Moral-Rubio, S. Muñoz Romero, and J.-L. Rojo-Álvarez, "On the black-box challenge for fraud detection using machine learning (I): Linear models and informative feature selection," Appl. Sci., vol. 12, no. 7, p. 3328, Mar. 2022, doi: 10.3390/app12073328.

Cite this article:

Rajeswari I & Premalatha N, "Credit Card Fraud Detection", Journal of Multidimensional Research and Review (JMRR), Vol.6, Iss.2, pp.61-69, 2025