Grenze International Journal of Engineering and Technology, January Issue

Foresight: Advanced Algorithms for Detecting Plastic Money Fraud

Maitrayee Kakandwar[1] and Sheetal Kulkarni[2]
[1-2]MIT-WPU, Pune, India
Email: maitrayee.kakandwar@mitwpu.edu.in, sheetal.kulkarni@mitwpu.edu.in

***Abstract*—The widespread adoption of plastic money, such as credit and debit cards, for online payments has made financial systems increasingly vulnerable to fraud attempts by cybercriminals. Safeguarding financial security requires effective detection and mitigation of such fraudulent transactions. Machine learning offers a powerful solution for this challenge by identifying suspicious patterns within transaction data. This paper investigates the use of various machine learning models—including Convolutional Neural Networks (CNN), Random Forest, Naïve Bayes, and Artificial Neural Networks (ANN)—to categorize transactions as either fraudulent or genuine. Furthermore, the study explores enhanced accuracy and detection capabilities achieved by combining two models in a hybrid approach. This strategy enables financial institutions to proactively detect and address fraudulent activities, strengthening overall system security. The findings highlight the significant potential of machine learning in advancing fraud detection, ultimately fostering a safer and more dependable digital financial environment.**

***Index Terms*— CNN, Machine Learning, Big Data CNN, ANN, Random Forest, Naive Bayes.**

I. INTRODUCTION

In today's digital age, cyberspace has revolutionized how individuals and organizations engage with financial services. The convenience of accessing financial platforms and conducting transactions via the internet has significantly impacted the global economy. However, alongside these benefits, there has been a corresponding rise in challenges, particularly in the form of cyber threats. One of the most prominent risks is the increasing incidence of online fraud, especially related to the use of credit and debit cards, often referred to as "plastic money." As more individuals adopt these payment methods for activities such as online shopping, net banking, and other digital transactions, cybercriminals are continually identifying new ways to exploit system vulnerabilities and steal sensitive financial information.

Online card fraud, including unauthorized transactions and identity theft, poses a significant threat to both consumers and financial institutions. Cybercriminals use increasingly advanced methods to gain access to sensitive financial data, resulting in monetary losses, as shown in Figure 1, and reduced trust in digital payment systems. Globally, the growing frequency of plastic money fraud has emerged as a major concern for businesses and government agencies. The widespread impact of such fraud highlights the urgent need for effective security measures and intelligent detection systems to safeguard financial ecosystems.

Machine learning algorithms have proven to be an effective tool in addressing the escalating threat of financial fraud by enabling the detection and prevention of unauthorized transactions.

Grenze ID: 01.GIJET.12.1.56_1

These algorithms can process large volumes of transaction data in real time, demonstrating strong capabilities in recognizing fraudulent patterns and distinguishing between legitimate and suspicious activities. By training models on historical data, machine learning systems can learn the behavioral patterns and characteristics of both typical and fraudulent activities. This ability to identify anomalies makes them well-suited for early detection of potential fraud.

Several machine learning algorithms, including Convolutional Neural Networks (CNN), Random Forest [1], Naïve Bayes [2], and Artificial Neural Networks (ANN) [2], have been successfully applied in fraud detection. While CNN is primarily used for image recognition, it can also be adapted to analyze transaction patterns. Random Forest and Naïve Bayes are commonly employed for classification tasks due to their ability to handle large datasets with high accuracy. Meanwhile, ANN, with its complex structure, can model non-linear relationships in data, making it effective in identifying subtle patterns that traditional methods might overlook.

Machine learning algorithms are tailored to analyse transactional data and detect potential fraud by examining key factors like transaction amount, location, and time. These models assess the likelihood of a transaction being fraudulent, enabling faster identification of suspicious activities after deployment. Integrating machine learning into fraud detection marks a major step forward in combating the rising threat of cybercrime in the financial sector. As cyber threats evolve, adopting more advanced and intelligent data-driven approaches is essential to ensure the security and reliability of financial transactions across digital platforms.

Figure 1. Plastic-Money Fraud Data

II. Literature Review

The detection of financial fraud, particularly in plastic money transactions, has been extensively studied using a variety of machine learning (ML) and deep learning (DL) approaches. Research has demonstrated the use of ensemble and neural network-based models, such as Random Forest, Long Short-Term Memory (LSTM), and Convolutional Neural Networks (CNN) [3][7], which have shown promise in capturing complex fraud patterns. However, a consistent limitation across several works is the scarcity of real-world datasets [1], which constrains the ability to build models with robust generalization capabilities. Studies combining Artificial Neural Networks (ANN) and Naïve Bayes with Genetic Algorithm (GA) for feature selection [8] have highlighted the challenge of reproducibility, as results often vary when tested on different datasets [5]. Additionally, models incorporating CNN, Recurrent Neural Networks (RNN), and LSTM have faced interpretability challenges and susceptibility to data drift [3], emphasizing the need for adaptive models capable of evolving with fraud patterns.

To address data imbalance and improve robustness, some studies have integrated adaptive synthetic sampling techniques with CNN [4], demonstrating the benefits of training on diverse datasets. The use of Synthetic Minority Over-Sampling Technique (SMOTE) combined with CNN and Autoencoders [5] has also yielded improved detection rates, but the complexity of network architectures and the lack of variable interpretability have hindered practical deployment. Multi-Layer Perceptron (MLP) models paired with CNN [6] have attempted to counter imbalanced data issues [4]; however, optimal accuracy remains difficult to achieve. While certain frameworks have successfully identified emerging fraud patterns, their adaptability to continuously evolving customer behaviors remains limited [7]. Sparse Autoencoders coupled with Generative Adversarial Networks (GANs) [8] have shown encouraging results but presented stability and implementation concerns. Likewise, SVM, Logistic Regression, and CNN combinations [9] have improved class imbalance handling but still leave room for accuracy enhancements.

Emerging techniques, such as Variational Autoencoders (VAEs) [10], offer promising capabilities for anomaly detection but face challenges in interpreting latent spaces and ensuring clear separation between normal and anomalous instances. Unsupervised learning strategies have also been applied for highly imbalanced datasets, contributing to performance gains in scenarios with limited labeled data [13]. Overall, the reviewed literature highlights that while ML and DL techniques have significantly advanced fraud detection capabilities, key limitations—such as handling severe class imbalance, ensuring interpretability, and adapting to dynamic fraud behaviors—persist. Addressing these challenges will be critical to developing next-generation fraud detection systems capable of reliable real-world deployment.

III. Research Gap

Based on the literature review, the field of fraud detection using deep learning and machine learning models still faces several critical challenges. Despite the implementation of advanced algorithms and techniques in various studies, a significant issue remains the limited generalizability of these models when applied to diverse, real-world datasets. Additionally, interpretability challenges continue to hinder stakeholders' ability to comprehend how decisions are made during fraud detection processes. The performance limitations of models utilizing Synthetic Minority Over-Sampling Technique (SMOTE) [5] were also noted, highlighting difficulties in handling class imbalances. A notable gap identified in the current research is the models' inability to effectively adapt to emerging fraud patterns and evolving customer behaviors. Furthermore, some studies reported issues related to model stability, especially concerning performance metrics. Future research should focus on developing models that are both interpretable and adaptable, capable of operating efficiently with limited real-world data while maintaining accuracy in dynamic and evolving environments.

IV. Dataset

The dataset used in this study was obtained from a publicly available source on Kaggle titled "Fraud Detection". It contains a comprehensive collection of anonymized transaction records designed to simulate real-world financial activities. The dataset comprises over 550,000 transaction entries stored in the file, each annotated with attributes such as transaction time, amount, merchant category, and location, along with a binary label indicating whether the transaction was fraudulent. This labelled structure enables effective training and evaluation of supervised machine learning models. The dataset offers a balanced mix of categorical and numerical features, making it suitable for testing various algorithms under realistic financial conditions. Its scale and diversity provide a strong foundation for developing robust fraud detection systems.

V. Methodology

The proposed methodology integrates advanced machine learning techniques within a structured framework to address the limitations identified in the literature review. The system architecture consists of four major stages: data preprocessing, feature selection and analysis, model training, and prediction refinement. Figure. 2 (System Architecture) illustrates the complete workflow, where the dataset is first cleaned, transformed, and balanced before being passed to the Random Forest (RF) [21] model for feature importance ranking and preliminary classification. The selected features are then fed into a Multi-Layer Perceptron (MLP) [6] model, which captures deeper non-linear relationships and refines predictions. The final stage outputs the fraud probability, supported by evaluation metrics for accuracy, recall, and ROC-AUC performance.

A. Model Description

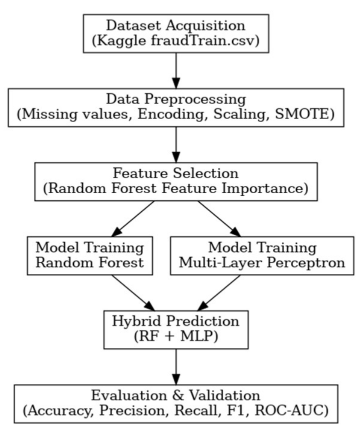

Figure 2. System Architecture of The Model

Random Forest is a robust ensemble learning technique that builds multiple decision trees during training and combines their predictions using majority voting. Its ability to handle high-dimensional, structured data [4] makes it well-suited for fraud detection tasks.

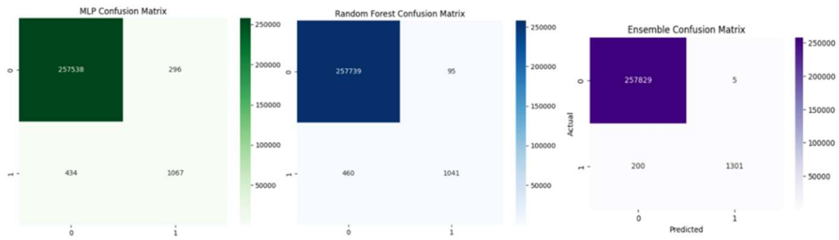

Figure 3. Confusion Matrix of RF, MLP & Ensemble Models

The Multi-Layer Perceptron is a deep learning architecture consisting of an input layer, one or more hidden layers, and an output layer, with each neuron connected via weighted edges. Leveraging non-linear activation functions such as ReLU or sigmoid, and trained using backpropagation, MLPs excel at modelling complex, non-linear relationships in data.

The proposed hybrid model strategically combines the strengths of both algorithms. Random Forest is employed for feature reduction and to generate reliable initial predictions, ensuring the model starts from a strong, interpretable foundation. These outputs are then refined by the MLP, which adapts to dynamic and non-linear fraud patterns for enhanced accuracy. This integration not only boosts overall detection performance but also ensures a balance between interpretability and adaptability, crucial for real-world financial fraud detection.

B. System Architecture

The proposed system architecture is designed as a hybrid learning pipeline comprising five interconnected layers. The Data Ingestion Layer is responsible for loading the financial transaction dataset and conducting initial exploration to understand its structure and distribution. The Preprocessing and Feature Engineering Layer addresses missing values, encodes categorical variables, applies normalization, and mitigates class imbalance using techniques such as SMOTE [22]. In the Modelling Layer, two independent models are trained: Random Forest, chosen for its high interpretability and robust feature selection [20] capabilities, and Multi-Layer Perceptron (MLP), selected for its ability to capture deep, non-linear patterns within the data. The Hybrid Integration Layer then combines either the predictions or selected features from the Random Forest with the MLP's learned representations to refine classification outcomes. Finally, the Evaluation Layer rigorously compares the performance of individual and hybrid models using established metrics

C. Why This Approach is Superior

Traditional single model approaches often face a trade-off between interpretability and adaptability. Random Forest is strong in explainability and structured-data performance, but less flexible for dynamic, evolving fraud patterns. MLP, while powerful in detecting complex relationships, is prone to overfitting and requires extensive tuning. The proposed hybrid system capitalizes on RF's stability and MLP's adaptability, ensuring higher recall for rare fraudulent cases without sacrificing precision. By blending statistical robustness with deep learning flexibility, the framework offers improved generalization, resilience to data imbalance, and better adaptability to emerging fraud tactics—making it more effective for real-world deployment.

VI. RESULTS

TABLE. I. COMBINED CLASSIFICATION REPORT

Metric	RF	MLP	Ensemble
Accuracy	0.9979	0.9972	0.9992
AUC Score	0.9885	0.9862	0.9999
Precision (Class1)	0.92	0.78	1.00
Recall (Class 1)	0.69	0.71	0.87
F1-Score (Class 1)	0.79	0.75	0.93
Macro Avg F1	0.89	0.87	0.96
Weighted Avg F1	1.00	1.00	1.00

The performance of Random Forest, MLP, and an Ensemble model was evaluated using various metrics to identify fraudulent transactions effectively. Confusion matrices, classification reports, and ROC curves were analysed to assess accuracy, precision, recall, F1-score, and AUC. While both Random Forest and MLP performed well, the ensemble approach demonstrated superior performance by achieving the highest recall and AUC scores. This indicates a better capability in identifying minority class (fraudulent) transactions, making the ensemble model more robust and reliable for fraud detection tasks.

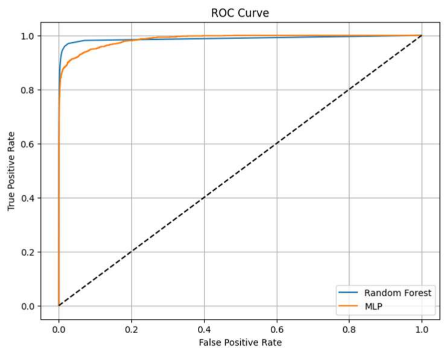

Figure 4. ROC Curve of Random Forest and MLP

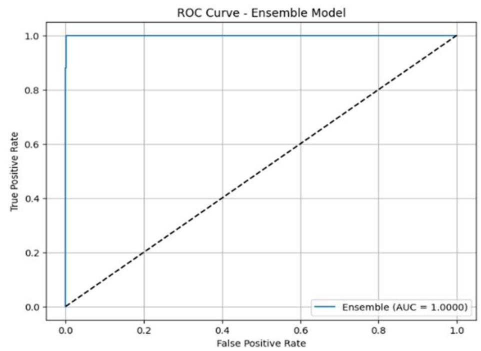

Figure 5. ROC Curve of Ensemble Model

The ensemble model outperformed individual classifiers, achieving an AUC of 0.9999 compared to 0.9885 (Random Forest) and 0.9862 (MLP). Its recall for the fraud class improved to 0.87, surpassing Random Forest (0.69) and MLP (0.71). The ensemble also achieved the highest F1-score of 0.93, reflecting balanced and accurate fraud detection as shown in the Table 1.

The confusion matrices, as shown in Figure 3, show that the ensemble model had the lowest false positives (5) and false negatives (200), outperforming both Random Forest and MLP. While Random Forest and MLP misclassified 460 and 434 fraudulent transactions respectively, the ensemble model correctly identified more fraud cases, demonstrating improved accuracy and reliability in detecting fraudulent activities.

The ROC, shown in Figure 3 and Figure 4, curves illustrate the superior performance of the ensemble model, which achieved an AUC of 1.0, indicating perfect discrimination between classes. In comparison, the Random Forest and MLP models also performed well but with slightly lower AUCs. The ensemble's near-vertical curve and top-left alignment highlight its exceptional ability to detect fraudulent transactions accurately.

VII. CONCLUSION

In conclusion, the detection of plastic money fraud—such as credit and debit card fraud—remains a pressing challenge in the financial sector, particularly with the exponential growth of online transactions. This project explored the use of machine learning and deep learning techniques to address this issue, implementing Random Forest, MLP, and an ensemble model to classify fraudulent transactions from a large dataset. Among these, the ensemble model outperformed individual classifiers, achieving a near-perfect AUC and significantly higher recall for the minority fraud class. This highlights the strength of hybrid models in handling class imbalance and improving fraud detection accuracy. However, despite promising results, challenges persist. Issues like model interpretability, adaptability to novel fraud strategies, and maintaining stability across diverse transaction patterns still hinder real-world deployment. Models such as CNNs, Autoencoders, and ensemble techniques offer potential, but their generalization and transparency must improve. Going forward, developing adaptive, explainable, and resilient fraud detection systems will be crucial for securing digital payment platforms, enhancing user trust, and minimizing financial losses.

REFERENCES

[1] Prasad, R. Dev, G. Shobha and J. Shetty, "Machine Learning Techniques to Detect Fraud in Credit Cards on the HPCC Systems Platform," 2019 4th International Conference on Computational Systems and Information Technology for Sustainable Solution (CSITSS), Bengaluru, India, 2019, pp. 1-7, doi: 10.1109/CSITSS47250.2019.9031032.

[2] 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

[3] D. Mienye and N. Jere, "Deep Learning for Credit Card Fraud Detection: A Review of Algorithms, Challenges, and Solutions," in IEEE Access, vol. 12, pp. 96893-96910, 2024, doi: 10.1109/ACCESS.2024.3426955.

[4] M. L. Gambo, A. Zainal and M. N. Kassim, "A Convolutional Neural Network Model for Credit Card Fraud Detection," 2022 International Conference on Data Science and Its Applications (ICoDSA), Bandung, Indonesia, 2022, pp. 198-202, doi: 10.1109/ICoDSA55874.2022.9862930.

[5] Z. Zhang and S. Huang, "Credit Card Fraud Detection via Deep Learning Method Using Data Balance Tools," 2020 International Conference on Computer Science and Management Technology (ICCSMT), Shanghai, China, 2020, pp. 133-137, doi: 10.1109/ICCSMT51754.2020.00033.

[6] A. A. El Naby, E. El-Din Hemdan and A. El-Sayed, "Deep Learning Approach for Credit Card Fraud Detection," 2021 International Conference on Electronic Engineering (ICEEM), Menouf, Egypt, 2021, pp. 1-5, doi: 10.1109/ICEEM52022.2021.9480639.

[7] Benchaji, I., Douzi, S., El Ouahidi, B. et al. Enhanced credit card fraud detection based on attention mechanism and LSTM deep model. J Big Data 8, 151 (2021). https://doi.org/10.1186/s40537-021-00541-8

[8] J. Chen, Y. Shen and R. Ali, "Credit Card Fraud Detection Using Sparse Autoencoder and Generative Adversarial Network," 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 2018, pp. 1054-1059, doi: 10.1109/IEMCON.2018.8614815.

[9] F. K. Alarfaj, I. Malik, H. U. Khan, N. Almusallam, M. Ramzan and M. Ahmed, "Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms," in IEEE Access, vol. 10, pp. 39700-39715, 2022, doi: 10.1109/ACCESS.2022.3166891.

[10] F. Alshameri and R. Xia, "An Evaluation of Variational Autoencoder in Credit Card Anomaly Detection," in Big Data Mining and Analytics, vol. 7, no. 3, pp. 718-729, September 2024, doi: 10.26599/BDMA.2023.9020035.

[11] Vanini, P., Rossi, S., Zvizdic, E. et al. Online payment fraud: from anomaly detection to risk management. Financ Innov 9, 66 (2023). https://doi.org/10.1186/s40854-023-00470-w

[12] Leevy, J.L., Hancock, J. & Khoshgoftaar, T.M. Comparative analysis of binary and one-class classification techniques for credit card fraud data. J Big Data 10, 118 (2023). https://doi.org/10.1186/s40537-023-00794-5

[13] Kennedy, R.K.L., Salekshahrezaee, Z., Villanustre, F. et al. Iterative cleaning and learning of big highly-imbalanced fraud data using unsupervised learning. J Big Data 10, 106 (2023). https://doi.org/10.1186/s40537-023-00750-3

[14] Alzubaidi, L., Zhang, J., Humaidi, A.J. et al. Review of deep learning: concepts, CNN architectures, challenges, applications, future directions. J Big Data 8, 53 (2021). https://doi.org/10.1186/s40537-021-00444-8

[15] Swiderski, B., Osowski, S., Gwardys, G. et al. Random CNN structure: tool to increase generalization ability in deep learning. J Image Video Proc. 2022, 3 (2022). https://doi.org/10.1186/s13640-022-00580-y

[16] K. J and A. Senthilselvi, "Detection of Credit Card Fraud Detection Using HPO with Inception Based Deep Learning Model," 2023 5th International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 2023, pp. 70-77, doi: 10.1109/ICIRCA57980.2023.10220771.

[17] V. R. Adhegaonkar, A. R. Thakur and N. Varghese, "Advancing Credit Card Fraud Detection Through Explainable Machine Learning Methods," 2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), Bengaluru, India, 2024, pp. 792-796, doi: 10.1109/IDCIoT59759.2024.10467999.

[18] H. Aldosari, "Garra Rufa Fish Optimization-based K-Nearest Neighbor for Credit Card Fraud Detection," 2024 International Conference on Distributed Computing and Optimization Techniques (ICDCOT), Bengaluru, India, 2024, pp. 1-5, doi: 10.1109/ICDCOT61034.2024.10516188.

[19] B. Paulraj, "Machine Learning Approaches for Credit Card Fraud Detection: A Comparative Analysis and the Promise of 1D Convolutional Neural Networks," 2024 7th International Conference on Information and Computer Technologies (ICICT), Honolulu, HI, USA, 2024, pp. 82-92, doi: 10.1109/ICICT62343.2024.00020.

[20] M. M. Khaled and Z. AL Aghbari, "ccfDetector: Utilizing GAN and Deep Learning for Credit Card Fraud Detection," 2023 Advances in Science and Engineering Technology International Conferences (ASET), Dubai, United Arab Emirates, 2023, pp. 1-6, doi: 10.1109/ASET56582.2023.10180825.

[21] M. Z. Mizher and A. B. Nassif, "Deep CNN approach for Unbalanced Credit Card Fraud Detection Data," 2023 Advances in Science and Engineering Technology International Conferences (ASET), Dubai, United Arab Emirates, 2023, pp. 1-7, doi: 10.1109/ASET56582.2023.10180615.

[22] M. N. Yousuf Ali, T. Kabir, N. L. Raka, S. Siddikha Toma, M. L. Rahman and J. Ferdaus, "SMOTE Based Credit Card Fraud Detection Using Convolutional Neural Network," 2022 25th International Conference on Computer and Information Technology (ICCIT), Cox's Bazar, Bangladesh, 2022, pp. 55-60, doi: 10.1109/ICCIT57492.2022.10054727.

[23] M. Z. Mizher and A. B. Nassif, "Deep CNN approach for Unbalanced Credit Card Fraud Detection Data," 2023 Advances in Science and Engineering Technology International Conferences (ASET), Dubai, United Arab Emirates, 2023, pp. 1-7, doi: 10.1109/ASET56582.2023.10180615.

[24] S. M. Gopavaram and P. Vinothiyalakshmi, "Cloud Based Credit Card Fraud Detection System in Banking Using Machine Learning and Deep Learning algorithms," 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), Delhi, India, 2023, pp. 1-4, doi: 10.1109/ICCCNT56998.2023.10307070.

[25] Kennedy, R.K.L., Villanustre, F., Khoshgoftaar, T.M. et al. Synthesizing class labels for highly imbalanced credit card fraud detection data. J Big Data 11, 38 (2024). https://doi.org/10.1186/s40537-024-00897-7