Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 46 (2025), No. 2, pp. 521–530
DOI : 10.47974/JIOS-1932

Advancing financial security : A hybrid fusion of neural network and rule-based system for credit card fraud detection

A. Krishna Chaitanya *
Department of Computer Science and Engineering (Cyber Security)
Institute of Aeronautical Engineering
Dundigal
Hyderabad 500043
Telangana
India

S. Satheesh †
Department of Electronics and Communication Engineering
RV Institute of Technology
Chebrolu
Guntur 522212
Andhra Pradesh
India

R. Raja Kumar §
Department of Computer Science and Engineering
Rajeev Gandhi Memorial College of Engineering and Technology
Nandyal 518501
Andhra Pradesh
India

A. Rajyalakshmi ‡
Department of Computer Science and Engineering
K G Reddy college of Engineering
Chilkur Village, Moinabad Mandal
Hyderabad 500075
Telangana
India

---

* *E-mail:* **chaituit2004@gmail.com (Corresponding Author)**
† *E-mail:* **surthanis22@gmail.com**
§ *E-mail:* **rajakumar.rajaboina@gmail.com**
‡ *E-mail:* **rajya.moses@gmail.com**

K. Lakshmi Abhigyna [@]
Department of Computer Science and Engineering (Cyber Security)
Institute of Aeronautical Engineering
Dundigal
Hyderabad 500043
Telangana
India

E. Surya Teja [#]
Department of Computer Science and Engineering (Cyber Security)
Institute of Aeronautical Engineering
Dundigal
Hyderabad 500043
Telangana
India

T. Nikhil [$]
Department of Computer Science and Engineering (Cyber Security)
Institute of Aeronautical Engineering
Dundigal
Hyderabad 500043
Telangana
India

Abstract

Credit card fraud presents a serious threat to financial institutions, causing substantial financial and reputational damage. To address this, the proposed method combines a neural network with a rule-based system to enhance fraud detection. This hybrid model effectively examines credit card transactions by capturing complex patterns and integrating expert insights, improving accuracy and minimizing false positives. By leveraging human-understandable rules and domain knowledge, the approach enhances transparency in decision-making processes. This innovative solution represents a significant advancement in fraud detection, helping financial institutions mitigate losses while ensuring greater trust and security in financial transactions.

Subject Classification: *68T05, 68T10.*

Keywords: *Neural networks, Rule-based systems, Hybrid model, Credit card fraud detection.*

[@] *E-mail:* **abhikaranam04@gmail.com**
[#] *E-mail:* **suryatejaeasari@gmail.com**
[$] *E-mail:* **nikhilkanna30@gmail.com**

1. Introduction

The increasing use of credit cards has led to higher transaction volumes and a rise in fraudulent activities, making fraud detection a critical challenge for financial institutions. Traditional methods like neural networks often struggle with interpretability and false positives [8]. Recent advancements, such as Random Forest algorithms, have improved detection speed and accuracy [2], while deep neural networks excel at identifying complex transaction patterns [3]. Preprocessing and algorithm selection significantly impact fraud detection performance [10].

In response, the proposed hybrid approach combines neural network precision with rule-based transparency, reducing false positives and enhancing interpretability. By integrating domain-specific knowledge, this method enables better real-time fraud monitoring and decision-making. Figure 1 illustrates the upward trend in credit card users and transaction volumes over recent years.

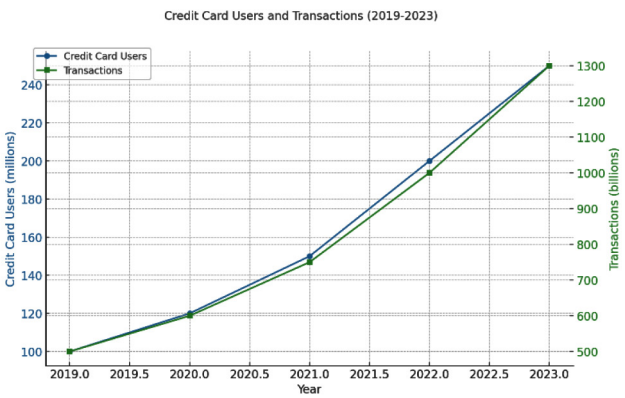

Figure 1

Growth Graph

2. Literature Review

T. Jemimah Jebaseeli [2] introduced an unsupervised Random Forest algorithm that enhanced fraud detection speed and accuracy but showed limited applicability beyond credit card transactions.

Xiaohan Yu [11] proposed a deep neural network method that improved accuracy and reduced manual feature engineering but faced challenges with scalability, computational efficiency, and decision-making transparency.

S. P. Maniraj [9] emphasized preprocessing, visualization, and anomaly detection but overlooked ethical concerns like data privacy and bias.

Dejan Varmedja [10] highlighted the importance of preprocessing and algorithm selection but lacked validation in real-world fraud detection scenarios.

S. KSRK [5] proposed the LGDCB framework, improving texture classification and offering solutions for fraud detection.

N. Perveen et al. [6] developed a dynamic kernel-based approach, enhancing fraud detection by adapting to changing patterns.

K. R. Prasad [7] highlighted the role of distributed computing in scaling fraud detection systems for large datasets.

3. Existing Method

Deep neural network models play a crucial role in credit card fraud detection, leveraging their ability to process vast data and extract intricate patterns without explicit feature engineering [3]. Techniques like log transform and focal loss address data skewness and hard examples during training [11]. However, their lack of transparency makes it difficult to interpret flagged transactions [4]. Additionally, these models require extensive preprocessing and parameter tuning, which can be resource-intensive [9]. They also struggle to incorporate domain-specific knowledge, potentially missing critical fraud patterns [8].

4. Problem Statement

- Current fraud detection methods, primarily based on neural networks, lack of transparency and understanding among stakeholders due to the complex nature of the models.
- Conventional fraud detection systems may produce a high number of false positives, resulting in unnecessary inconvenience for legitimate cardholders and increased operational costs for financial institutions.
- Current fraud detection methods may not provide comprehensive analysis and interpretation of credit card transactions, hindering informed decision-making in fraud prevention efforts.

- Existing fraud detection systems may struggle to accurately identify fraudulent transactions, potentially leading to financial losses and reputational harm for financial institutions.

5. Proposed Method

The proposed method combines a neural network with a rule-based system to improve credit card fraud detection. By integrating domain knowledge and human-understandable rules, this hybrid model enhances transparency and enables a more comprehensive transaction analysis. It captures intricate patterns and expert insights, providing a robust solution without claiming superiority over existing methods. The objectives of the proposed method are:

1. Enhance transparency in fraud detection by incorporating human-understandable rules through the rule-based system.
2. Minimize false positives in fraud detection results by combining neural network capabilities with domain-specific knowledge embedded in rule-based systems.
3. In order to provide thorough analysis and interpretation of credit card transactions, integrate neural networks with rule-based systems to enable better informed decision-making in fraud detection procedures.
4. Increase fraud detection accuracy by leveraging the complementary strengths of a neural network with a rule-based system to identify complex patterns.

6. Methodology

6.1 *Hybrid Fusion*

To achieve the outlined objectives, a hybrid fusion involving a neural network as well as a rule-based system is applied in the fraud detection process. The neural network predicts fraud, which is further analyzed by the rule-based system with domain-specific rules. This approach improves accuracy, reduces false positives, and offers transparent insights for better decision-making. The method involves the following steps:

6.1.1 Data Collection and Preprocessing

The IEEE CIS 2019 dataset, available on Kaggle ("*https://www.kaggle.com/competitions/ieee-fraud-detection/data*"), is used in both the training and testing of the model [11]. The dataset includes 519,000 transactions, with 80% for training and 20% for testing. It features transaction details, card information, and anonymized data derived from PCA to preserve user privacy. Preprocessing methods applied include scaling numerical features, encoding categorical variables, handling missing values. Addressing class imbalance using SMOTE (Synthetic Minority Oversampling Technique) [1]. Table 1 outlines the dataset features, their descriptions, and types.

Table 1
Features Table

Data Type	Feature Details
Categorical	**isFraud**: Indicates whether the transaction is fraudulent. **card1 – card6**: Information related to the card used in the transaction. **addr1 – addr2**: Address details associated with the transaction. **M1 - M9**: Anonymized features related to the transaction. **P_emaildomain**: The email domain of the purchaser. **R_emaildomain**: The email domain of the receiver.
Numerical	**TransactionAmt**: The monetary value of the transaction. **dist1 – dist 2**: Geographical distance between transaction locations. **C1 – C14**: Anonymized numerical features derived from the data. **D1 – D15**: Additional set of anonymized numerical features. **V1 – V339**: A further set of anonymized features used for transaction analysis.
Time/ID	**TransactionID:** A unique identifier for the transaction. **TransactionDT:** The timestamp of the transaction, indicating when it occurred.

6.1.2 Neural Network Model Development

The neural network consists of Input, Hidden, and Output layers with dense connections, ReLU activation in hidden layers, and sigmoid in the output for binary classification. Dropout regularization (0.4 for hidden, 0.5 for input layers) and batch normalization stabilize training. A learning rate of 0.0005 ensures steady convergence. The model is optimized using

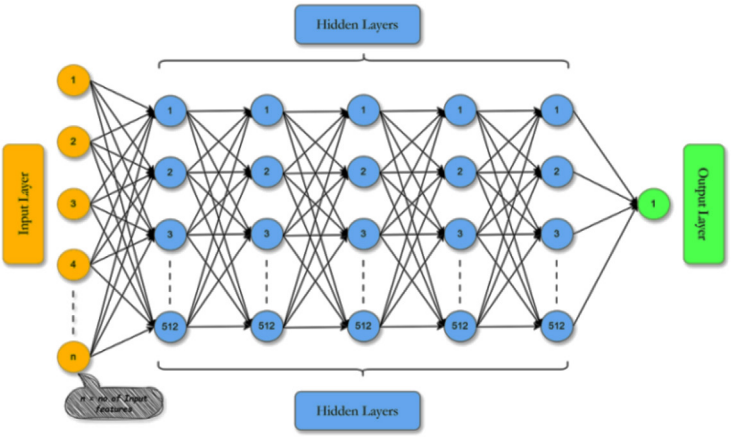

Figure 2

Overview of the Neural Network Model

backpropagation and the Nadam optimizer, which combines Nesterov and RMSprop for improved convergence. The binary cross-entropy loss function guides optimization by comparing predicted probabilities with actual outcomes. The Nadam optimizer adjusts the learning rate for efficient training. Figure 2 illustrates the overall design of the neural network model.

The model starts with random weights and biases, and during the forward pass, input data generates predictions using the neural network function *f*, computed as

$$\hat{y}_i = f(x_i; W, b)$$

ReLU activation functions are applied to introduce non-linearity. The binary cross-entropy loss is calculated as

$$L = \frac{1}{N} \Sigma_{i=1}^{N} \mathcal{L}(\hat{y}_i, y_i)$$

where $\mathcal{L}$ denotes the chosen loss function. Backpropagation updates parameters using Nadam, and EarlyStopping and ReduceLROnPlateau prevent overfitting, tracking metrics over 20 epochs.

6.1.3 Development of Rule-Based System

The rule-based system employs specific thresholds and patterns, such as transaction amounts, frequencies, locations, and spending behaviors, to detect fraud. It combines neural network model predictions

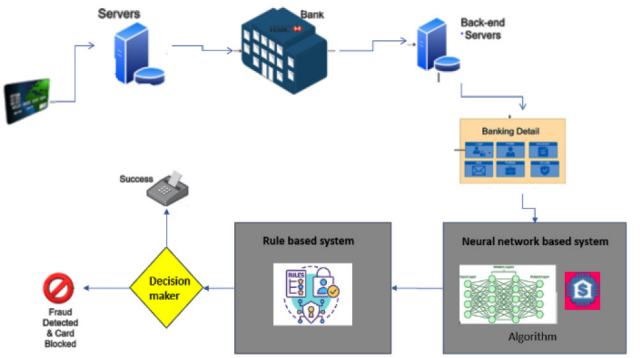

Figure 3

Integrated and Sequential Processing Pipeline

with transaction history and account details for a holistic analysis, implemented via Python functions with conditional logic.

6.1.4 Integration and Sequential Processing

The neural network model and rule-based system are combined in a sequential pipeline. Neural network model outputs guide the rule-based analysis, ensuring accurate, transparent decisions and reducing false positives. Figure 3 illustrates the data flow from financial institutions to the decision-making stage.

6.1.5 Evaluation

This evaluation measures the accuracy of the fraud detection system by comparing its predictions against truth labels.

$$\text{Accuracy} = \frac{\text{Correct Predictions}}{\text{Total Predictions}}$$

7. Implementation

The fraud detection system prepares the dataset by splitting it into training and testing sets, followed by preprocessing (scaling, imputing missing values, one-hot encoding). The neural network is trained with early stopping and learning rate reduction to prevent overfitting. A rule-based system analyzes the model's output using predefined rules. Both systems are integrated into a sequential pipeline, with performance evaluated using accuracy.

8. Results

The hybrid model achieved an impressive 98.41% accuracy, surpassing traditional models like Naïve Bayes, Logistic Regression, and SVM. Table 2 presents the accuracy values of various models, with data for the other models sourced from [11].

9. Conclusion and Future Scope

The hybrid method combining neural networks and rule-based systems enhances credit card fraud detection by improving accuracy and reducing false positives. It leverages neural network pattern recognition and the interpretability of rule-based systems, offering transparency and adaptability to evolving fraud patterns. This solution improves security, reduces operational costs, and overcomes limitations of traditional methods, protecting both institutions and customers.

Future work can optimize the neural network and refine the rule-based system for better performance. Real-time implementation and expansion into other domains, like insurance claims or online retail, could further enhance its impact. As credit card usage grows, this method ensures secure transactions and builds customer trust.

References

[1] A. Fernandez, S. Garcia, F. Herrera, and N. V. Chawla, "SMOTE for Learning From Imbalanced Data: Progress and Challenges, Marking the 15-year Anniversary," *Journal of Artificial Intelligence Research*, vol. 61, pp. 863–905, Apr. (2018), doi: 10.1613/jair.1.11192.

[2] T. J. Jebaseeli, R. Venkatesan, and K. Ramalakshmi, "Fraud Detection for Credit Card Transactions Using Random Forest Algorithm," in *Advances in intelligent systems and computing*, pp. 189–197 (2020). doi: 10.1007/978-981-15-5285-4_18.

[3] Z. Kazemi and H. Zarrabi, "Using Deep Networks for Fraud Detection in the Credit Card Transactions," *Proceedings of IEEE 4th International Conference on Knowledge-Based Engineering and Innovation*, pp. 0630–0633, Dec. (2017), doi: 10.1109/kbei.2017.8324876.

[4] J. Kumar and V. Saxena, "Rule-Based Credit Card Fraud Detection Using User's Keystroke Behavior," in *Lecture notes in networks and systems*, pp. 469–480 (2022). doi: 10.1007/978-981-19-0707-4_43.

[5] S. KSRK, "Local Gradient Dual Coding Book (LGDCB) Framework for Effective Texture Classification," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 6, no. 4, pp. 1680–1687, Aug. (2019), doi: 10.30534/ijatcse/2019/95842019.

[6] N. Perveen, D. Roy, and K. M. Chalavadi, "Facial expression recognition in videos using dynamic kernels," *IEEE Transactions on Image Processing*, vol. 29, pp. 8316–8325, Jan. (2020), doi: 10.1109/tip.2020.3011846.

[7] K. R. Prasad, "Big Data sentiment Analysis using Distributed Computing approach," in *Advances in intelligent systems and computing*, pp. 689–699 (2018). doi: 10.1007/978-981-13-1580-0_66.

[8] A. Pumsirirat and L. Yan, "Credit Card Fraud Detection Using Deep Learning Based on Auto-Encoder and Restricted Boltzmann Machine," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 1, Jan. (2018), doi: 10.14569/ijacsa.2018.090103.

[9] T. R. Pillai, I. A. T. Hashem, S. N. Brohi, S. Kaur, and M. Marjani, "Credit Card Fraud Detection Using Deep Learning Technique," *Proceedings of 4th International Conference on Advances in Computing, Communication and Automation*, pp. 1–6, Oct. (2018), doi: 10.1109/icaccaf.2018.8776797.

[10] D. Varmedja, M. Karanovic, S. Sladojevic, M. Arsenovic, and A. Anderla, "Credit Card Fraud Detection - Machine Learning methods," *18th International Symposium INFOTEH-JAHORINA (INFOTEH)*, Mar. (2019), doi: 10.1109/infoteh.2019.8717766.

[11] X. Yu, X. Li, Y. Dong, and R. Zheng, "A Deep Neural Network Algorithm for Detecting Credit Card Fraud," *International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE)*, Jun. (2020), doi: 10.1109/icbaie49996.2020.00045.

Received November, 2024