ISSN: 2582-7219

International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Impact Factor: 8.206

Volume 8, Issue 4, April 2025

© 2025 IJMRSET | Volume 8, Issue 4, April 2025| DOI:10.15680/IJMRSET.2025.0804287

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Advancing Financial Security: A Hybrid Fusion of Neural Networks and Rule-Based System for Credit Card Fraud Detection

T. Teja Kumar Reddy, M. Goutham, N. Goutham Reddy, D. Goutham Sai, S. Govind Reddy

Students, Department of Artificial Intelligence and Machine Learning (AI&ML), Malla Reddy University, Maisammaguda, Hyderabad, India

Prof. S. Ashok

Department of Artificial Intelligence and Machine Learning (AI&ML), Malla Reddy University, Maisammaguda, Hyderabad, India

ABSTRACT: In the current landscape, credit card fraud poses a substantial threat to financial institutions, resulting in significant financial losses and reputational damage. The sophistication of modern fraud techniques, including stolen card information, identity theft, and unauthorized transactions, exacerbates the challenge. The proposing method introduces an innovative strategy for credit card fraud detection by merging neural networks with rule-based systems. The objective is to address the significant challenges faced by financial institutions. By fusing neural networks with rule-based systems, a hybrid model is created that allows for a thorough examination of credit card transactions, capturing complex patterns and utilizing expert insights. This integration enhances the transparency of decision- making processes by incorporating domain knowledge and human-understandable rules. Overall, the proposed approach represents a significant advancement in fraud detection, offering a comprehensive solution that helps financial institutions mitigate losses and enhance trust and security in their transactions.

I. LITERATURE REVIEW

[1] T. Jemimah Jebaseeli (2021) developed an unsupervised random forest algorithm that reduced the number of fraud transactions. This enhancement improved the speed of online transactions and overall system accuracy. However, the applicability of this algorithm beyond credit card transactions remains limited.

[2] Xiaohan Yu (2020) proposed a comprehensive approach using a deep neural network algorithm. This approach effectively improved detection accuracy and reduced the need for manual feature engineering. However, it failed to address potential scalability challenges or computational efficiency issues associated with deploying the proposed deep neural network algorithm in large-scale production environments. One significant drawback is their lack of transparency in decision- making, making it challenging to understand the rationale behind flagged transactions.

[3] Dejan Varmejda (2019) evaluated various machine learning algorithms for credit card fraud detection. The study emphasized the importance of preprocessing and algorithm selection. However, it lacked external validation or comparison with real-world fraud detection systems or industry benchmarks.

[4] S P Maniraj (2019) proposed an approach involving dataset preprocessing, data visualization techniques, and anomaly detection algorithms. However, ethical and legal implications, including data privacy concerns and potential biases, were not adequately addressed.

II. PROPOSED WORK

In contrast, the proposed system presents an innovative approach to credit card fraud detection by integrating neural network with rule-based system. This hybrid model seeks to overcome the shortcomings of the existing system implicitly. By combining the strengths of both methodologies, the system enhances transparency in decision-making

© 2025 IJMRSET | Volume 8, Issue 4, April 2025| DOI:10.15680/IJMRSET.2025.0804287

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

implicitly by incorporating domain knowledge and human-understandable rules implicitly. Moreover, it facilitates a more comprehensive analysis of credit card transactions, capturing nuanced patterns and leveraging expert insights implicitly. This implicit approach ensures a more robust fraud detection framework without explicitly mentioning the pro-posed system's superiority over the existing one. Overall, the proposed approach represents a significant advancement in fraud detection, offering a holistic solution to mitigate the limitations of the existing methods implicitly. The objectives of the proposed method are: 1. Ensure that the fraud detection process is understandable and transparent to stakeholders by incorporating human- understandable rules by using 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. Facilitate more informed decision-making in fraud detection processes by integrating neural networks and rule-based systems to provide comprehensive analysis and interpretation of credit card transactions. 4. Increase the accuracy of fraud detection by leveraging the strengths of both neural networks and rule-based systems to capture complex patterns and expert insights.

III. IMPLEMENTATION OF PROPOSED WORK

The implementation of the fraud detection system involves several key steps, integrating both the neural network model and the rule-based system to ensure robust fraud detection. The following steps outline the process:

1. Data Loading and Preparation: The dataset containing transaction details is loaded, and the features and the target variable (isFraud) are separated. The data is then split into training and testing sets to facilitate model training and evaluation.

2. Data Preprocessing: Identify categorical and numerical features in the dataset. Apply appropriate preprocessing steps, including imputing missing values in numerical features with a constant value and scaling the features. For categorical features, impute missing values with the most frequent value and apply one- hot encoding. Additionally, ensure numerical features are scaled appropriately and address any imbalances in the data.

3. Model Training and Evaluation: Preprocess the training data before defining the neural network model architecture. Utilize callbacks for early stopping and learning rate reduction to prevent overfitting and optimize convergence. Preprocess the testing data using the same pipeline as the training data. Evaluate the trained model's performance on the testing set by predicting probabilities of fraudulent transactions. Figure 8 depicts the code snippet for training the neural network model.

Figure 1: Code for NN Model Training

4. Rule-Based System: Implement a rule-based system to analyze the output of the model and apply predefined rules for further analysis. Define rules based on thresholds and patterns indicative of fraud, such as transaction amount, frequency, location, and spending behavior. provides a code snippet representing the function and conditions defined within the rule-based system.

© 2025 IJMRSET | Volume 8, Issue 4, April 2025| DOI:10.15680/IJMRSET.2025.0804287

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

IV. ARCHITECTURE

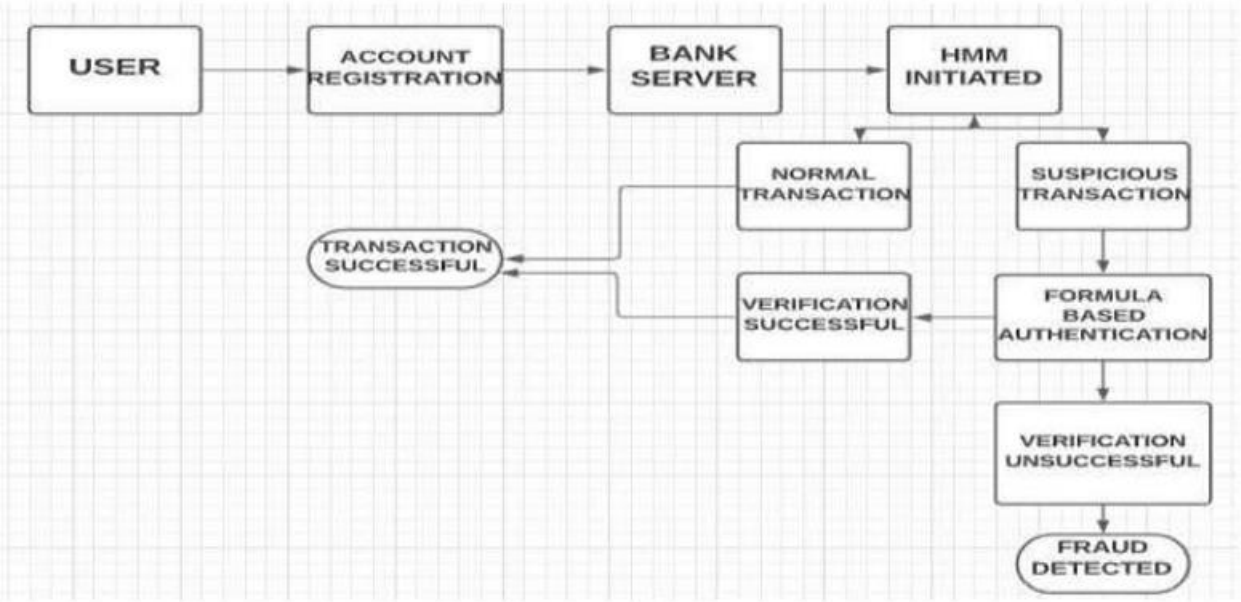

Fig 4.2.1 Fraud Detection System Architecture

V. RESULTS AND DISCUSSION

The developed Hybrid model achieved an impressive accuracy of 98.41% as shown in figure 16, outperforming other models trained on the same dataset. The model's accuracy surpasses that of traditional machine learning algorithms such as Naïve Bayes, Logistic Regression, and SVM, indicating its effectiveness in detecting fraudulent transactions. Table 3 provides a comparison of model performance, showcasing the superiority of the neural network approach. Figure 11 shows the performance comparison of different models based on their accuracy. Accuracy details in Table 3 and Figure 11 are sourced from [17], providing insights into the performance of various models in detecting fraudulent transactions.

Table 3: Models Performance Comparison

Model	Accuracy
Naïve Bayes	0.875
Logistic Regression	0.911
SVM	0.932
Neural Network (NN)	0.954
NN (with focal loss)	0.957
Hybrid Model	0.984

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

VI. CONCLUSION

The proposed method successfully integrates neural networks with rule-based systems to enhance credit card fraud detection. By leveraging the pattern recognition capabilities of neural networks and the interpretability and domain knowledge embedded in rule-based systems, the hybrid model achieves improved detection accuracy and a significant reduction in false positives. The method's transparency in decision-making processes and adaptability to evolving fraud patterns provide a robust tool for financial institutions, enhancing security and reducing operational costs associated with managing fraudulent transactions. This integration addresses the limitations of traditional neural network-based methods and offers a scalable solution to safeguard against fraudulent activities, protecting both institutions and their customers.

Future Scope: Looking ahead, future scope can focus on optimizing the neural network architecture and refining the rule-based system for even better performance. Exploring real- time implementation will enable immediate fraud detection and prevention in transaction processing environments. Additionally, investigating the applicability of this hybrid approach in other domains, such as insurance claims or online retail transactions, can further extend its impact. As credit card usage and transaction volumes continue to rise, the proposed method provides an effective and adaptable solution to combat fraud, ensuring the security and reliability of financial transactions while maintaining and building customer trust.

REFERENCES

[1] Mubarek, A., & Adalı, E. (2017). Multilayer Perceptron Neural Network Technique for Fraud Detection. Proceedings of International Conference on Computer Science and Engineering, Antalya.
[2] Kazemi, Z., & Zarrabi, H. (2017). Using Deep Networks for Fraud Detection in The Credit Card Transactions. Proceedings of IEEE 4th International Conference on Knowledge-Based Engineering and Innovation, Tehran.
[3] Awoyemi, J. O., Adetunmbi, A. O., & Oluwadare, S. A. (2017). Credit card fraud detection using machine learning techniques: A comparative analysis. 2017 International Conference on Computing Networking and Informatics (ICCNI).
[4] Yee, O. S., Sagadevan, S., & Malim, N. H. A. H. (2018). Credit card fraud detection using machine learning as data mining technique. Figure 11: Models Accuracy Comparison Graph Journal of Telecommunication, Electronic and Computer Engineering (JTEC), 10(1-4), 23- 27.
[5] Pumsirirat, A., & Yan, L. (2018). Credit Card Fraud Detection using Deep Learning based on Auto-Encoder and Restricted Boltzmann Machine. International Journal of Advanced Computer Science and Applications, 9(1).
[6] Dhankhad, S., Mohammed, E., & Far, B. (2018). Supervised machine learning algorithms for credit card fraudulent transaction detection: a comparative study. IEEE International Conference on Information Reuse and Integration (IRI), 122-125.
[7] Lakshmi, S., & Kavilla, S. (2018). Machine Learning for Credit Card Fraud Detection System. International Journal of Applied Engineering Research, 13(24), 16819-16824.
[8] Pillai, T., Hashem, I., Brohi, S., Kaur, S., & Marjani, M. (2018). Credit Card Fraud Detection Using Deep Learning Technique. Proceedings of 4th International Conference on Advances in Computing, Communication and Automation, Subang Jaya.
[9] Wang, S., Liu, G., Li, Z., Xuan, S., Yan, C., & Jiang, C. (2018). Credit Card Fraud Detection Using Capsule Network. Proceedings of IEEE International Conference on Systems, Man, and Cybernetics, Miyazaki.
[10] Roy, A., et al. (2018). Deep Learning Detecting Fraud in Credit Card Transactions. Presented at the 2018 Systems and Information Engineering Design Symposium (SIEDS). DOI: 10.1109/sieds.2018.8374722.
[11] Zamini, M., & Montazer, G. (2018). Credit Card Fraud Detection Using Autoencoder Based Clustering. Proceedings of 9th International Symposium on Telecommunications, Tehran.
[12] Jiang, Changjun et al. (2018). Credit Card Fraud Detection: A Novel Approach Using Aggregation Strategy and Feedback Mechanism. IEEE Internet of Things Journal, 5, 3637-3647.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com