Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 16, Issue. 1: 2025
ISSN : **1906-9685**

HYBRID DEEP LEARNING MODEL FOR UPI FRAUD DETECTION USING CNN AND RANDOM FOREST

L. Dhana Lakshmi Assistant Professor, Department of CSE, Seshadri Rao Gudlavalleru Engineering College, Gudlavalleru, Andhra Pradesh. dhanayarlagadda@gmail.com
B. Sravanthi, A. Sugun Pandu Raju, B.Gayathri Sadvika, B.Venu Nayak, UG Student, Department of CSE, Seshadri Rao Gudlavalleru Engineering College, Gudlavalleru, Andhra Pradesh. bussasravanthi2004@gmail.com

Abstract: With the increasing adoption of Unified Payments Interface (UPI) transactions, fraud has surged, posing a significant risk to users and financial institutions. Traditional fraud detection methods often struggle to keep pace with evolving attack patterns, leading to false positives and missed fraudulent cases. To address this, we propose a hybrid deep learning model that combines Convolutional Neural Networks (CNN) and Random Forest (RF) to improve fraud-detection accuracy. In this study, CNN was used to extract high-level transactional patterns and capture complex relationships within the financial data. The extracted features are then classified using RF, which enhances interpretability and robustness. The dataset used consists of real-world UPI transactions preprocessed using standard scaling and noise reduction techniques to improve generalization. The proposed model was trained and evaluated using a balanced dataset to mitigate class imbalance issues. The experimental results demonstrate that the proposed CNN-RF model achieves high accuracy while maintaining a low false-positive rate. Compared to standalone models, this hybrid approach significantly enhances fraud-detection efficiency. This study highlights the importance of combining deep learning with traditional machine learning techniques for real-time fraud detection in digital payments. Future work will include the integration of real-time anomaly detection and adaptive learning techniques to further enhance security.

Keywords: UPI fraud detection, hybrid deep learning, convolutional neural network. Random Forest Classification, Digital Payment Security.

1. **Introduction**

The evolution of digital payment systems has transformed financial transactions by offering users seamless, fast, and secure payment options[1]. Among these innovations, the Unified Payments Interface (UPI) has emerged as a game changer in the fintech industry, enabling instant fund transfers with minimal transaction costs[2]. The ease of use, real-time settlement, and interoperability between different banks and payment service providers have contributed significantly to the widespread adoption of UPI. However, with the rapid increase in UPI transactions, there has been a parallel increase in fraudulent activities, posing severe security threats to consumers and financial institutions. Fraudsters have become increasingly sophisticated, leveraging tactics, such as phishing scams, social engineering attacks, fake UPI applications, malware injections, and identity theft, to deceive users and manipulate digital payment systems. Traditional fraud-detection mechanisms, including rule-based and static machine learning models, often fail to identify these evolving threats[3]. Many of these systems rely on predefined thresholds and fixed behavioral patterns, making them less effective for detecting new fraud techniques[4]. Moreover, the high false-positive rates in conventional fraud-detection frameworks create unnecessary disruptions in legitimate transactions, impacting user experience and financial operations.

https://doi.org/10.36893/JNAO.2025.V16.I01.026

To address these challenges, this study proposes a hybrid fraud-detection model that integrates Convolutional Neural Networks (CNNs) for deep feature extraction and Random Forest (RF) for robust classification[5]. CNNs are highly efficient in detecting intricate transaction patterns and capturing subtle anomalies that rule-based systems might overlook. However, deep learning models alone may lack interpretability, which is why the RF classifier is introduced as a decision-making component **to** ensure enhanced transparency and accuracy in fraud detection[6]. The proposed CNN-RF framework is designed to minimize false positives while maintaining high fraud-detection accuracy, thereby improving overall transaction security[7]. By combining the pattern recognition strengths of deep learning with the robustness of ensemble learning, this approach offers a more adaptive and effective solution for detecting fraudulent UPI transactions in real time. This study explored the effectiveness of this hybrid model through rigorous experimentation and evaluation, aiming to enhance financial security and reduce fraud-related risks in digital payment ecosystems.

2. Literature Review

2.1 Traditional Fraud Detection Approaches

Fraud detection in financial transactions has been a critical area of research and various methods have been employed over time[8]. Traditional rule-based systems rely on predefined heuristics and manually crafted rules to flag suspicious transactions[9]. Although these methods work well for identifying known fraud patterns, they struggle to adapt to new and evolving fraud techniques. Moreover, rule-based systems generate a large number of false positives, leading to disruptions in legitimate transactions. Statistical methods such as linear regression and anomaly detection models have also been applied to fraud detection[10]. These techniques analyze transactional trends and flag deviations based on historical data. However, their effectiveness is often limited when dealing with large-scale high-dimensional datasets that are commonly found in modern financial transactions.

2.2 Machine Learning-Based Fraud Detection

To overcome the limitations of traditional models, machine learning algorithms such as Support Vector Machines (SVM), Decision Trees, and Logistic Regression have been widely explored[11]. These models can analyze transaction features and classify fraudulent patterns more efficiently. However, one of the significant challenges faced by machine learning-based fraud detection is dealing with imbalanced datasets, where fraudulent transactions make up only a small fraction of the overall data[12]. This imbalance often results in biased models that fail to effectively detect fraud.

2.3 Deep Learning and Hybrid Models

Recent advances in deep learning have introduced CNNs as powerful tools for fraud detection[13]. CNNs can extract deep features from transaction data and identify hidden fraud patterns that traditional models may miss[14]. However, standalone CNN models can suffer from overfitting and difficulties in handling the structured tabular data. To address these challenges, researchers have integrated random forests (RF) with CNN to create hybrid models. RF, an ensemble learning technique, enhances classification accuracy and provides interpretability. By combining CNN’s feature extraction capability with RF robustness, hybrid models achieve higher fraud detection accuracy, reducing both false positives and false negatives.

2.4 Existing research works

Naikl et al. [15] highlighted the transformative role of AI and Machine Learning in enhancing the UPI security. Their study emphasized how fraud-detection systems powered by deep learning can identify anomalies in real-time. They concluded that adaptive AI models are essential for combating evolving fraud techniques and improving financial transaction security. Sindhu and Swarupa [16] emphasized the rising fraud risk in UPI transactions due to increased online payment usage. Their research introduced a Hidden Markov Model (HMM)-based fraud-detection system**,** where deviations from a trained model indicate fraudulent activity. They evaluated multiple machine learning techniques, including auto-encoder, K-means clustering, and local outlier factors**,** to enhance fraud detection accuracy. Their study highlights the challenges of public data accessibility, class imbalance, and evolving fraud patterns. The authors stress that an efficient fraud detection system is crucial for financial institutions to minimize losses and enhance transaction security. Gupta et al. [17] explored UPI-based financial fraud detection using deep learning techniques to enhance security in digital transactions. Their study demonstrated how neural networks analyze transaction patterns to detect fraudulent behavior. They highlighted the importance of real-time fraud detection and emphasized the superiority of deep learning over traditional rule-based methods in identifying evolving fraud tactics. Charan and Thilak [18] focused on detecting phishing links and QR code fraud in UPI transactions by using machine learning. Their study emphasized how fraudsters manipulate links and QR codes to deceive users. By applying ML algorithms, they improved the detection accuracy, helping to enhance UPI security and effectively reduce unauthorized transactions.

2.5 Literature Gap

Existing fraud-detection models, including rule-based systems and machine-learning techniques, struggle with evolving fraud patterns and imbalanced datasets. While deep learning models, such as CNNs, improve detection accuracy, they often suffer from overfitting and computational challenges. Hybrid approaches, such as CNN with Random Forest, show promise, but research lacks real-time implementation and adaptability to emerging fraud tactics.

3. Methodology

3.1 Dataset Details

The dataset used in this study consists of real-world UPI transaction records that capture the various transactional attributes necessary for fraud detection. It includes details, such as sender and receiver IDs, transaction amounts, timestamps, and fraud labels, which indicate whether a transaction is legitimate or fraudulent. The dataset represents a mix of both normal and suspicious transactions, making it suitable for training and evaluating fraud detection models. To ensure accuracy and reliability, the dataset underwent preprocessing steps, including the removal of inconsistencies, handling missing values, and standardizing the numerical features**.** Feature scaling is applied to normalize transaction amounts, and categorical data, such as sender and receiver IDs, are encoded for better model interpretation. Since fraudulent transactions are significantly fewer than legitimate transactions, balancing techniques are used to ensure that the model does not become biased. This clean and structured dataset helps improve the effectiveness of the CNN-RF hybrid model in detecting UPI fraud.

3.2 Data Preprocessing

Data pre-processing is a crucial step before training the model to enhance the accuracy and efficiency of fraud detection. The dataset was first examined for missing values, which were handled using statistical imputation techniques to ensure completeness and to prevent data loss. Next, feature scaling is applied to transaction amounts and other numerical fields using a standard scalar to bring all values to a uniform range. This helps to prevent larger numerical values from disproportionately influencing the model's predictions. Because UPI transactions include categorical data, such as sender and receiver IDs, these values are encoded to convert them into numerical representations that the model can process efficiently. Additionally, there are significantly fewer fraudulent transactions than legitimate transactions, leading to an imbalanced dataset. To address this, oversampling techniques are used to create a more balanced distribution, allowing the CNN-RF hybrid model to effectively detect fraud without bias toward legitimate transactions.

3.3 Hybrid Model Architecture

The proposed model integrates a CNN for feature extraction and an RF for classification.

3.3.1 CNN Feature Extraction:

The Convolutional Neural Network (CNN) plays a crucial role in extracting meaningful patterns from UPI transaction data, allowing the model to effectively detect fraud. The process begins with an input layer that uses normalized transaction data to ensure that all features are within a consistent range (Fig. 1). This step prevents extreme values from skewing model predictions. Subsequently, convolutional layers were applied to extract spatial and sequential patterns from the transaction sequences. These layers use filters to detect important relationships between different transaction attributes, such as sender-receiver behavior and transaction frequency. The activation functions in these layers help to highlight fraudulent patterns that may not be easily recognizable through traditional methods. Finally, the extracted feature maps are flattened into a structured format using a flattened layer.

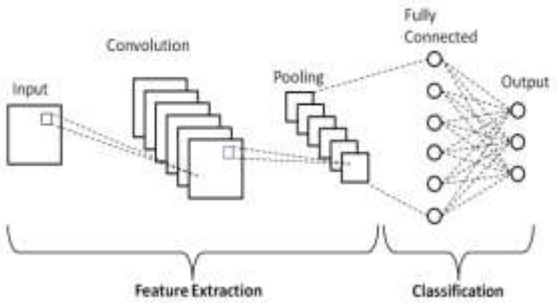


Fig. 1 Basic architecture of CNN[19]

This step transforms multidimensional data into a single vector, making it ready for classification using the Random Forest model, which ultimately determines whether a transaction is fraudulent or legitimate.

3.3.2 Random forest (RF) classification

Once the CNN extracts transaction features, they are passed to the Random Forest (RF) model for the final classification. The RF is an ensemble learning method that combines multiple decision trees to obtain robust predictions, as shown in Fig. 2. By simultaneously analyzing multiple transaction attributes, RF effectively distinguishes between fraudulent and legitimate transactions. Each decision tree within the RF model evaluates different aspects of the transaction, such as the amount, sender-receiver behavior, and transaction-time patterns. This reduces the risk of overfitting, making the model more generalizable across various fraudulent scenarios. Additionally, RF provides high interpretability, allowing financial analysts to understand why a specific transaction is classified as fraudulent. Compared to standalone deep learning models, RF enhances reliability by combining feature extraction from a CNN with rule-based classification logic. This hybrid approach improves accuracy and minimizes false positives, making it a powerful fraud-detection solution for UPI transactions in real-world financial systems.

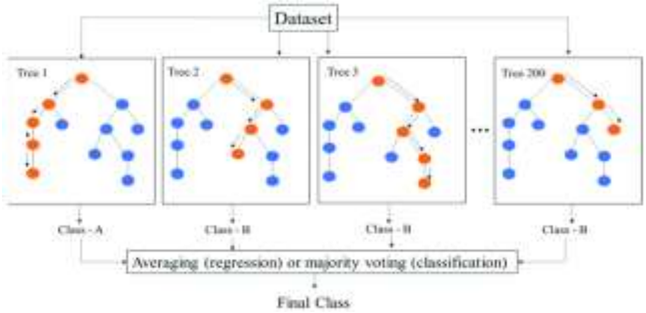


Fig. 2 Basic architecture of RF[20]

4. Results and discussions

4.1 Experimental Results

The effectiveness of the fraud detection model was evaluated using various performance metrics, including the accuracy, precision, recall, and ROC-AUC score. These metrics help to understand how well the model identifies fraudulent transactions while minimizing false positives and false negatives. A comparison between a standalone CNN model and the hybrid CNN + RF model demonstrated the advantage of combining deep learning with an ensemble learning technique. The standalone CNN model struggles with classification, achieving test accuracy of only 50% and an ROC-AUC score of 0.52, which indicates poor fraud detection capability. In contrast, the hybrid CNN+RF model significantly outperformed it, achieving a test accuracy of 99.7% and an ROC-AUC score of 99.99%**.**

Table 1 Performance Comparison

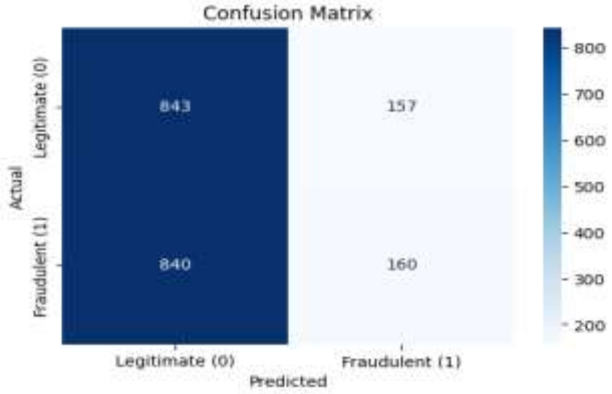
Model	**Test Accuracy**	**ROC-AUC Score**
Standalone CNN	50.0%	0.52
Hybrid CNN + RF	**99.7%**	**99.99%**

The results highlight the superiority of the CNN-RF hybrid approach in fraud detection, demonstrating better accuracy and reliability than a deep learning-only model.

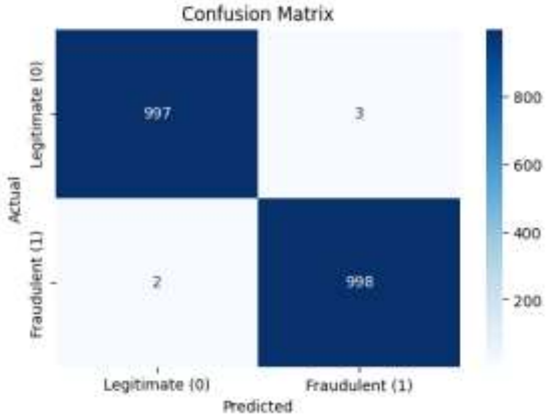
4.2 Confusion matrix

The confusion matrices illustrate the difference in performance between a standalone CNN model and a hybrid CNN-RF model for UPI fraud detection, as shown in Fig. 1 (a) and (b). In the Standalone

CNN Model (Fig. 1 (a)), the classifier struggled to distinguish between fraudulent and legitimate transactions, leading to a high number of misclassifications. The matrix reveals 843 true negatives (correct legitimate predictions) and 160 true positives (correct fraud detections), but the model also misclassifies 840 fraudulent transactions as legitimate, indicating a high false-negative rate. Similarly, 157 legitimate transactions were incorrectly classified as fraudulen**t**, resulting in unnecessary transaction blocks. The test accuracy of this model is approximately 50%, proving its inefficiency in fraud detection. In contrast, the CNN + RF Hybrid model (Fig. 1 (b)) demonstrated significant improvements. It achieved 997 true negatives and 998 true positives, with only three false positives and two false negatives. This marks a drastic reduction in misclassification rates**,** ensuring a more reliable fraud-detection system. The model attained a test accuracy of 99.7%**,** making it highly suitable for real-world applications in digital payment fraud prevention.



(a)



(b)

Fig. 1 (a) confusion matrix for CNN alone (b) confusion matrix for CNN + RF

4.3 Discussion and Challenges

The hybrid CNN-RF model significantly enhances fraud detection by leveraging the CNN's ability to capture deep transactional patterns and RF's interpretability of RF in classification. The model effectively reduces false negatives, ensuring that fewer fraudulent transactions remain undetected. Compared with standalone approaches, this hybrid technique minimizes misclassification errors and enhances fraud-detection reliability. The ROC-AUC score further confirmed the effectiveness of the model, showing its high sensitivity and specificity in identifying fraudulent activities. However, despite its excellent performance, some challenges persist. False positives, while minimized, remain an issue that leads to potential transaction blocks for legitimate users. In addition, the computational complexity increases owing to CNN feature extraction, impacting real-time processing efficiency. Another key challenge is the evolving nature of fraud, as fraudsters are constantly developing new techniques to bypass detection systems. This requires the continuous retraining and updating of the model to maintain its effectiveness in a dynamic financial environment.

5. Conclusion and Future Work

This study introduces an advanced hybrid fraud-detection framework that integrates CNN and RF to enhance the accuracy of fraud detection in UPI transactions. By leveraging CNN's capability of CNN to extract intricate transaction patterns and RF's strong classification ability of RF, the model significantly improves fraud detection performance. The experimental results demonstrate that the proposed approach surpasses traditional machine learning models, making it more reliable for practical implementation. The model effectively minimizes false positives and negatives, ensuring a higher level of security for digital financial transactions. Despite these promising results, there is scope for further research. Future research should focus on optimizing the model for real-time fraud detection in banking systems, allowing immediate intervention when fraudulent activity is detected. Additionally, incorporating adaptive learning techniques will help the model evolve continuously and adapt to emerging fraud tactics. Another critical direction is to enhance model transparency using Explainable AI (XAI) to provide clearer insights into fraud-classification decisions. By addressing these areas, this study contributes to the development of secure and intelligent financial transaction systems, reinforcing the need for hybrid AI models to detect fraudulent transactions more effectively.

References

[1] B. Ul, R. F., A. Mehraj, A. Ahmad, and S. Assad, "A Compendious Study of Online Payment Systems: Past Developments, Present Impact, and Future Considerations," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 5, pp. 256–271, 2017, doi: 10.14569/ijacsa.2017.080532.

[2] R. Kumar, "The evolution of banking through digital payment systems," *IJEETE J. Res.*, vol. 11, no. 2, pp. 284–295, 2024.

[3] J. Putrevu and C. Mertzanis, "The adoption of digital payments in emerging economies: challenges and policy responses," *Digit. Policy, Regul. Gov.*, vol. 26, no. 5, pp. 476–500, Jan. 2024, doi: 10.1108/DPRG-06-2023-0077.

[4] M. L. A. L. Dhaka, "The evolution of payment systems: from barter to digital transactions chandrakanth, dr. mohan lal dhaka," *Int J Adv FResearch Sci. Technol.*, vol. 11, no. 12, pp. 1678–1682, 2021.

[5] A. Kukkar, R. Mohana, A. Nayyar, J. Kim, B. G. Kang, and N. Chilamkurti, "A novel deep-learning-based bug severity classification technique using convolutional neural networks and random forest with boosting," *Sensors (Switzerland)*, vol. 19, no. 13, 2019, doi: 10.3390/s19132964.

[6] F. Khozeimeh *et al.*, "RF-CNN-F: random forest with convolutional neural network features for coronary artery disease diagnosis based on cardiac magnetic resonance," *Sci. Rep.*, vol. 12, no. 1, pp. 1–12, 2022, doi: 10.1038/s41598-022-15374-5.

[7] U. Knauer *et al.*, "Tree species classification based on hybrid ensembles of a convolutional neural network (CNN) and random forest classifiers," *Remote Sens.*, vol. 11, no. 23, 2019, doi: 10.3390/rs11232788.

[8] K. G. Al-Hashedi and P. Magalingam, "Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019," *Comput. Sci. Rev.*, vol. 40, p. 100402, 2021, doi: https://doi.org/10.1016/j.cosrev.2021.100402.

[9] Q. Liu, V. Hagenmeyer, and H. B. Keller, "A Review of Rule Learning-Based Intrusion Detection Systems and Their Prospects in Smart Grids," *IEEE Access*, vol. 9, pp. 57542–57564, 2021, doi: 10.1109/ACCESS.2021.3071263.

[10] W. Hilal, S. A. Gadsden, and J. Yawney, "Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances," *Expert Syst. Appl.*, vol. 193, p. 116429, 2022, doi: https://doi.org/10.1016/j.eswa.2021.116429.

[11] M. Bansal, A. Goyal, and A. Choudhary, "A comparative analysis of K-Nearest Neighbor, Genetic, Support Vector Machine, Decision Tree, and Long Short Term Memory algorithms in machine learning," *Decis. Anal. J.*, vol. 3, p. 100071, 2022, doi: https://doi.org/10.1016/j.dajour.2022.100071.

[12] V. Rodriguez-Galiano, M. Sanchez-Castillo, M. Chica-Olmo, and M. Chica-Rivas, "Machine learning predictive models for mineral prospectivity: An evaluation of neural networks, random forest, regression trees and support vector machines," *Ore Geol. Rev.*, vol. 71, pp. 804–818, 2015, doi: https://doi.org/10.1016/j.oregeorev.2015.01.001.

[13] Halima Oluwabunmi Bello, Adebimpe Bolatito Ige, and Maxwell Nana Ameyaw, "Deep learning in high-frequency trading: Conceptual challenges and solutions for real-time fraud detection," *World J. Adv. Eng. Technol. Sci.*, vol. 12, no. 2, pp. 035–046, 2024, doi: 10.30574/wjaets.2024.12.2.0265.

[14] I. D. Mienye and N. Jere, "Deep Learning for Credit Card Fraud Detection: A Review of

Algorithms, Challenges, and Solutions," *IEEE Access*, vol. 12, pp. 96893–96910, 2024, doi: 10.1109/ACCESS.2024.3426955.

[15] S. K. L. Naikl, A. Kiran, V. P. Kumar, S. Mannam, Y. Kalyani, and M. Silparaj, "Fraud Fighters - How AI and ML are Revolutionizing UPI Security," in *2024 International Conference on Science Technology Engineering and Management (ICSTEM)*, 2024, pp. 1–7. doi: 10.1109/ICSTEM61137.2024.10560740.

[16] V. S. S. Jallapuram Sindhu, "UPI FRAUD DETECTION USING MACHINE," *Int. J. Eng. Res. Sci. Tech.*, vol. 20, pp. 5–67, 2024.

[17] V. Gupta, S. Sharma, S. Nimkar, and S. Pathak, "UPI Based Financial Fraud Detection Using Deep Learning Approach," in *2024 International Conference on Advances in Computing Research on Science Engineering and Technology (ACROSET)*, 2024, pp. 1–6. doi: 10.1109/ACROSET62108.2024.10743663.

[18] G. R. Charan and K. D. Thilak, "Detection of Phishing Link and QR Code of UPI Transaction using Machine Learning," in *2023 3rd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*, 2023, pp. 658–663. doi: 10.1109/ICIMIA60377.2023.10426613.

[19] V. H. Phung and E. J. Rhee, "A High-accuracy model average ensemble of convolutional neural networks for classification of cloud image patches on small datasets," *Appl. Sci.*, vol. 9, no. 21, 2019, doi: 10.3390/app9214500.

[20] A. Khanal and M. F. Shahriar, "Physics-Based Proxy Modeling of CO2 Sequestration in Deep Saline Aquifers," *Energies*, vol. 15, no. 12, 2022, doi: 10.3390/en15124350.