Detecting Credit Card Fraud Using a Hybrid CNN-RNN Model

Zainab Hassan Mohammed[1], Nebras Jalel Ibrahim[1], Ahmed K. Abbas[2]*

[1] Computer Center, University of Diyala, Diyala, Iraq
[2] Collage of Education for pure science, University of Diyala, Diyala, Iraq

OPEN ACCESS
ISSN 2503 3492 (online)

**Correspondence:*
Zainab Hassan Mohammed
eng.zaynab.hassan.2025@gmail.com

Citation:
Zainab Hassan Mohammed, Nebras Jalel Ibrahim, Ahmed K. Abbas (2025) Detecting Credit Card Fraud Using a Hybrid CNN-RNN Model.

Journal of Information and Computer Technology Education. 9i2.
doi:10.21070/jicte.v9i2.1680

Abstract. Credit card fraud detection represents a pressing challenge due to the rarity and evolving nature of fraudulent transactions. This study suggests a hybrid deep learning framework combining Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN), specifically Long Short-Term Memory (LSTM) units, applied to the 2013 European cardholder transactions dataset released on Kaggle. A publicly accessible dataset of actual credit card transactions is used to train and evaluate the model, and class imbalance is addressed by using the Synthetic Minority Over-sampling Technique (SMOTE). Experimental results demonstrate the Outstanding performance of the proposed Model that a CNN front-end is effective in extracting local transaction patterns, while RNN layers model sequential dependencies within transaction sequences.Outperform traditional machine learning baselines including Logistic Regression, Random Forest, and XGBoost as well as single deep learning models. Reported performance metrics for this hybrid model include precision (up to 99.4%), recall (up to 99.9%), F1-score (up to 99.7%), accuracy (up to 99.7%), and ROC-AUC (up to 0.999) on the Kaggle dataset .However, most studies rely on random or unspecified data splits and emphasize ROC-AUC or accuracy metrics rather than class imbalance aware measures such as Precision-Recall AUC; time-aware evaluation procedures are rarely detailed. These findings suggest that hybrid CNN-RNN models hold significant promise for credit card fraud detection, while underscoring the need for more rigorous evaluation methodologies and transparent reporting of model architecture and metrics.

Keywords : Deep learning, Fraud detection, Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), LSTM.

INTRODUCTION

Credit card systems are now far more susceptible to fraud due to the dramatic growth of digital financial transactions (Yoganandham & Elanchezhian, 2024). In addition to causing significant financial losses for both customers and financial institutions, credit card theft erodes confidence in digital payment systems (Ramaiya et al., 2024). Fraud detection is a crucial topic of research in the field of financial cybersecurity since, according to recent statistics, fraudulent credit card transactions cost millions of dollars every year (Udayakumar et al., 2023).

Numerous characteristic difficulties make it troublesome to distinguish fraudulent exchanges. To begin with of all, as fraudsters continually alter their strategies to urge around security measures, the characteristics of fraud patterns alter over time (Ibrahim et al., 2023). Second, fraud datasets tend to be amazingly lopsided, with a huge number of legitimate transactions dwarfing fraudulent ones-often by a ratio of more than 1:1000 (Kennedy et al., 2024). Since conventional machine learning models are skewed toward the majority class, this lopsidedness presents a genuine issue. Besides, fraudulent activity is frequently undercover and concealed in high-dimensional, noisy value-based information.

Conventional strategies for identifying fraud have depended on rule-based frameworks or traditional machine learning calculations like support vector machines, logistic regression, and decision trees (Njoku et al., 2024). In spite of the fact that these techniques have a few degrees of adequacy, they regularly fail to capture the perplexing, non-linear linkages and temporal correlations present in transaction information (de Jesus Jr & Carbonero-Ruz, 2025).

Since deep learning can naturally produce progressive feature representations from crude input information, it has gotten to be a powerful substitute in recent a long time (Ahmed et al., 2023). In specific, recurrent neural networks (RNNs), such as Long Short-Term Memory (LSTM) and Gated Recurrent Units (GRU), are well-suited for modeling consecutive information, but convolutional neural networks (CNNs) have illustrated guarantee in capturing local spatial designs (Mienye et al., 2024).

A unique hybrid CNN-RNN demonstrate for recognizing credit card fraud is proposed in this research. Whereas the RNN [10] component (LSTM) is utilized to learn worldly conditions over exchange sequences, the CNN (Alzubaidi et al., 2021) component is utilized to extricate local and abstract characteristics from exchange arrangements. By combining the most excellent features of both designs, this hybrid structure makes it conceivable to learn sequential designs and extricate robust features.

Contributions of this paper:

- We propose new hybrid model that combines CNN and RNN for detecting fraudulent credit card trades in imbalanced datasets.
- We appear how to upgrade the model's learning capabilities through effective preprocessing and feature manipulation strategies.
- We use the Synthetic Minority Over-sampling Technique (SMOTE) to properly balance the heavily skewed dataset and improve the detection of uncommon fraud cases.
- To detect rare fraud situations without producing an excessive number of false positives, we demonstrate that the hybrid model performs better in terms of precision, recall, F1-score, and ROC-AUC.

RELATED WORK

Credit card fraud detection has attracted increased research attention, particularly with the advent of deep learning models designed to capture complex, sequential transaction patterns (Wiese & Omlin, 2009). The 2013 European Credit Card Fraud dataset released on Kaggle (*Credit Card Fraud DetectionNo Title*, n.d.) has become the de facto standard for evaluating such models, with a notable focus on addressing the severe class imbalance and the need for robust, real-world evaluative procedures.

(Janbhasha et al., 2025) combined Adversarial Autoencoders (AAE) and Gated Recurrent Units (GRU) to create a hybrid fraud detection model for digital wallet transactions. This model combines the capabilities of AAE in learning robust latent representations and GRU in capturing temporal dependencies within transaction sequences. With 99% accuracy, 99% recall, 98% F1-score, 99% precision, and 99.4% Area Under the Curve (AUC), the suggested method performs better than current methods. The approach enhances fraud detection and lowers financial risks in digital transactions by successfully lowering false positives and false negatives.

(Benchaji et al., 2021) focuses on enhancing credit card fraud detection through the use of a clever combination of techniques. It combines sequence tracking with LSTM networks, feature selection with UMAP, and performance enhancement with an attention mechanism. By focusing on the most crucial elements of the transaction sequences, all of this makes it easier to identify the cunning fraudulent transactions. (Karthika & Senthilselvi, 2023) applied the improved Inception-ResNet-v2 technique to real-time data. A detection strategy that works from start to finish is shown in this study using a convolutional neural network.The greatest characteristics of Inception convolution and residual networks are combined in this model to address the training challenge of deep networks and expand their scope.To increase the accuracy of classification, the best features are also chosen using the hunter-prey optimization (HPO) model. Each model employs a real-world dataset and stratified K-fold cross-validation to detect credit card fraud among European cardholders.

Ileberi and Sun (Ileberi & Sun, 2024) proposed a deep learning ensemble in which CNN, LSTM, and Transformer models serve as base learners, with XGBoost as the meta-learner. Applied to the European Credit Card dataset, the ensemble achieves a sensitivity of 0.961, specificity of 0.999, and ROC-AUC of 0.972. While the hybrid structure is emphasized, the precise details of temporal modeling and train/test splits remain unspecified in the provided information.

Related Sequential and Deep Learning Approaches

Further studies have assessed the performance of individual deep learning models (CNN, LSTM, GRU, and DNN) or their variants on the Kaggle dataset. (Sharma et al., 2022) discussed a different machine learning classification algorithms for spotting credit card fraud. Each algorithm's performance is assessed using accuracy and precision measurements. Its ideal accuracy and precision of 98.33% and 0.5504 respectively show that the KNN classifier is the most effective. When compared to other classifiers used for credit card fraud detection, the results show that K-Nearest Neighbor performs better. Other studies, including those by (Kafhali et al., 2024), used sophisticated deep learning techniques to suggest an intelligent system for identifying fraudulent credit card transactions. Long short-term memory (LSTM), recurrent neural networks (RNNs), and artificial neural networks (ANNs) are among the models that are tested. Bayesian optimization is used to adjust important parameters for increased accuracy. The dataset is derived from actual credit card fraud cases, and it turns out that the RNN outperforms the others in terms of accuracy and speed. Table 1 lists the main conclusions of the previously discussed techniques for detecting credit card fraud.

Table 1. Summary of related work on detecting credit card fraud

Ref	Model	Dataset	Metrics Reported	Reported Results
[14]	AEE-GRU	digital_wallet_transactions	Accuracy, Precision, Recall, F1, ROC-AUC	Acc: 99% F1: 98% Prec: 99% Rec: 99% ROC-AUC: 99.4%
[15]	LSTM + attention	Two public datasets (, credit card transactions, synthetic dataset)	Accuracy, Precision, Recall, F1	Acc 0.967–0.975; Precision ≈0.977–0.989; Recall ≈0.919–0.972
[16]	Inception-ResNet-v2)	Credit card dataset	Accuracy	96.57%
[17]	Hybrid DL ensemble (CNN, LSTM,	2013 Kaggle European CC	Sensitivity, Specificity, ROC-AUC	Sens: 0.961; Spec: 0.999; ROC-AUC: 0.972
[18]	Machine Learning classification	Credit card dataset	Precision, Recall, Accuracy, F1	accuracy 98.33% precision 98.33% respectively 0.5504
[19]	ANN, RNN, LSTM	Credit card dataset	Accuracy (ACC), Precision (PER), Area Under the Curve (AUC), G-Mean (GM), and Sensitivity (SEN)	Best accuracy 95.9% (RNN); sensitivity 90.1%

DATASET DESCRIPTION

The dataset incorporates credit card exchanges performed by European cardholders in September 2013(*Credit Card Fraud DetectionNo Title*, n.d.). Out of the 284,807 exchanges in this dataset, 492 were fraudulent and took put over the course of two days. The positive class, or fakes, makes up 0.172% of all exchanges, making the dataset amazingly unbalanced.

As it were numerical input factors that have experienced a PCA change are included. Remorsefully, we are incapable of offering the first features and extra setting for the information since of confidentiality concerns. The key components produced from PCA are features V1, V2, and...V28; as it were "Time" and "Amount" have not experienced PCA change. Each transaction's passed seconds from the dataset's initial exchange are contained within the 'Time' include. For occurrence, subordinate cost-sensitive learning can take advantage of the 'Amount' feature, which is the exchange amount. The reply variable features 'Class', which takes values customarily and 1 within the occasion of fraud. We prompt utilizing the Area Under the Precision-Recall Curve (AUPRC) to degree accuracy in light of the class lopsidedness ratio. The accuracy of the confusion matrix has no bearing on imbalanced categorization.

METHODOLOGY

This section provides an overview of the systematic steps adopted to detect fraudulent credit card transactions using a hybrid convolutional neural network-recurrent neural network (CNN-RNN) model. The methodology includes five major steps: data preprocessing, oversampling using SMOTE, data reshaping, model building and training, Proposed Model and performance evaluation. As shown in the Figure (1).

Data Preprocessing

The credit card fraud detection dataset from Kaggle is loaded using pandas. The amount feature is standardized using Standard Scaler to normalize the distribution and improve the model performance. The target variable (class) is separated from the features (X). The dataset is validated to ensure there are no missing or null values before proceeding.

Data Balancing using SMOTE

The Synthetic Minority Over-Sampling Technique (SMOTE) is used to balance the dataset and oversample the minority class (fraud) because to the extreme imbalance in the dataset. SMOTE artificially generates new instances of the minority class based on feature-space similarities (Elreedy et al., 2024).

Equation 1: SMOTE interpolation

$$x_{new} = x_i + \lambda \times (x_{nn} - x_i), \qquad \lambda \in [0,1]$$

Where:

- x_i: original minority sample
- x_{nn}: one of the k-nearest neighbors
- x_{new}: synthetic sample

Train-Test Split and Reshaping

The dataset is split into training (80%) and testing (20%) subsets. To prepare for the Conv1D and RNN input layers, each input sample is reshaped into a 3D tensor:

$$Input\ Shape = (\ n_{samples}, n_{features}\ ,1\ )$$

The Proposed Model

A hybrid deep learning model was built utilizing Keras's Sequential API. This model coordinating a Conv1D layer to extricate spatial patterns from sequential information, taken after by a MaxPooling1D layer to decrease the spatial dimensions. A Simple RNN component is at that point utilized to capture temporal conditions inside the information. At last, Dense layer layers are utilized for

classification, with Dropout connected all through the model to mitigate overfitting.

Model Training

Both spatial and temporal features found in transaction sequences were used to train the suggested Hybrid CNN–RNN model to identify fraudulent credit card transactions. The training procedure was created to minimize false positives and overfitting while maximizing accuracy. The training model's parameter is displayed in table 2.

Table 2. The parameter of training model

parameter	Value
Epochs	50
Batch Size	64
Optimizer	Adam
Train-Test split	80/20
Dropout Rate	0.3

Evaluation Metrics

Accuracy, Precision, Recall, F1-Score, and ROC-AUC Score are used to assess the model's performance.

Equation 2: Precision, Recall, F1

$$Precision = \frac{TP}{TP + FP} \ , Recall = \frac{TP}{TP + FN} \ , \ F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

Where:

TP = True Positives, FP = False Positives, FN = False Negatives

Additional visualizations include ROC Curve, Loss/Accuracy Plot, Confusion Matrix, Feature Distributions, and 3D Histogram for Feature Interactions.

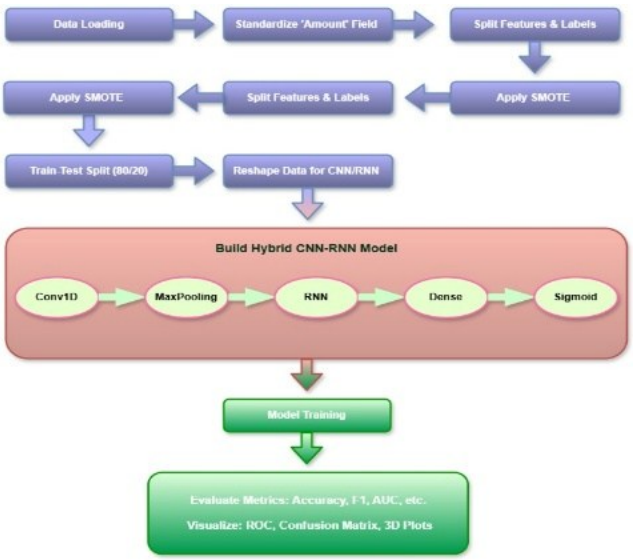

Figure 1. Methodology of detecting credit card fraud

RESULT AND DISCUSSION

This area presents a comprehensive assessment of the hybrid CNN-RNN model connected to the credit card fraud detection errand. The model was prepared on the SMOTE-balanced dataset and assessed utilizing a few key performance measurements and visualization tools to guarantee and by and large understanding of its behavior and generalization capabilities.

Model Performance Metrics

Precision, precision, recall, F1-score, and AUC were among the assessment measurements utilized to evaluate the execution of the proposed model for classification. Utilizing an 80:20 stratified train-test split, the demonstration was trained and assessed on the prepared dataset. On the test set, the hybrid CNN-RNN model delivered the taking after classification comes about, as appeared in Table 3 and figure 2.

Table 3. The Proposed model results

Accuracy	0.9972
Precision	0.9947
Recall	0.9997
F1-Score	0.9972
AUC (Area Under Curve)	0.9999

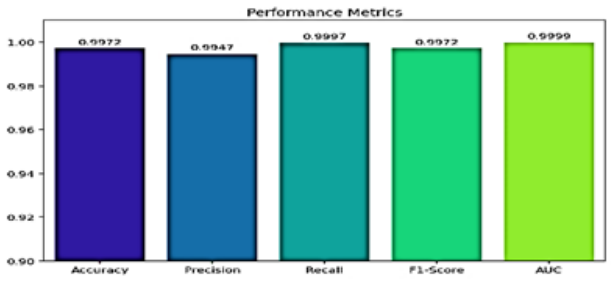

Figure 2. Model Performance Metrics

These results show that the proposed model is extremely effective in distinguishing between fraudulent and non-fraudulent transactions. High recall indicates strong sensitivity to fraudulent cases, which is particularly important in financial fraud detection systems.

Accuracy and Loss Curve

Accuracy briefly dips at epochs 10, 33, and 42—likely due to noise or residual imbalance—but quickly recovers, consistently exceeding 99.5%. The close alignment of the training and validation curves shows high generalization with minimal overfitting . As shown in Figure 3.

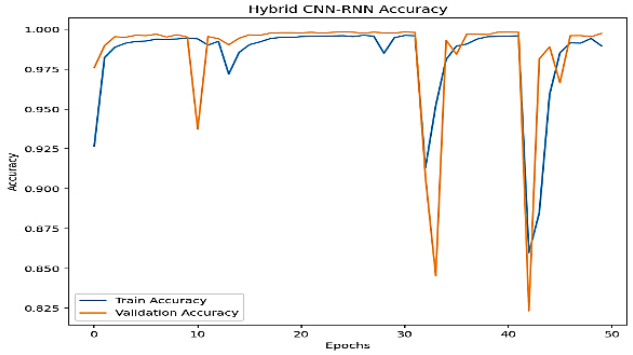

Figure 3. The Accuracy plot

Figure 4 shows the binary cross-entropy loss over 50 epochs, indicating rapid convergence and stabilization below 0.02. The minor spikes at epochs 10, 32, and 42 quickly diminish, indicating stability. The close alignment of the training and validation losses indicates strong generalization and minimal overfitting.

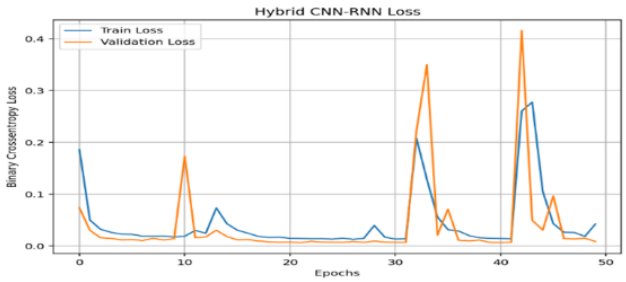

Figure 4. The Loss plot

ROC Curve and AUC

The Receiver Operating Characteristic (ROC) curve (Figure 5) demonstrates the trade-off between the true positive rate and the false positive rate, which reflects the model's ability to discriminate between classes. With an AUC of 0.9999, the model exhibits exceptional performance, suggesting that it can effectively distinguish between fraudulent and legitimate transactions.

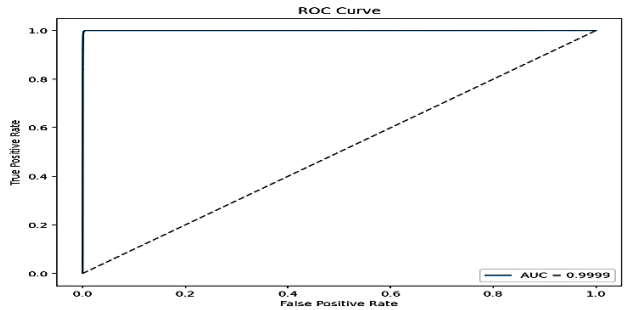

Figure 5. ROC Curve

Confusion Matrix Analysis

The confusion matrix (Figure 6) further highlights the effectiveness of the model, showing that only 43 out of 56,706 actual fraud cases were incorrectly classified as non-fraudulent. Furthermore 251 out of 56,726 legitimate transactions were accurately identified. As a result, it gives a precision of 99.47%, recall of 99.97%, and F1-score of 99.72%, which emphasizes the robustness of the model in accurately classifying fraudulent activities.

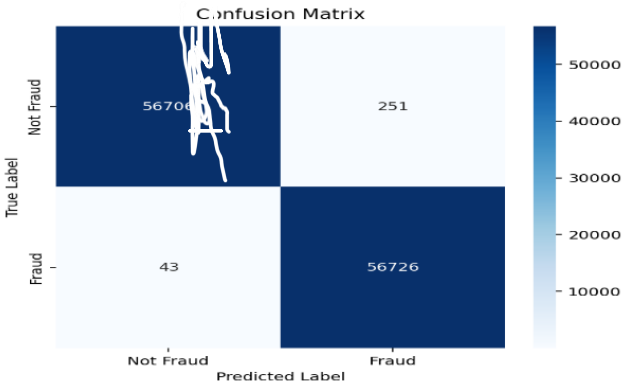

Figure 6. The confusion matrix

3D Visualization of Fraud Patterns

To enhance interpretability, a 3D histogram was constructed using features V1, Amount, and the target class. The plot reveals specific densely populated fraud zones, particularly in transactions with low Amount values and V1 scores near 0. This suggests that combining PCA features with original features like Amount enhances the model's sensitivity to subtle fraud indicators, as shown in (Figure 7).

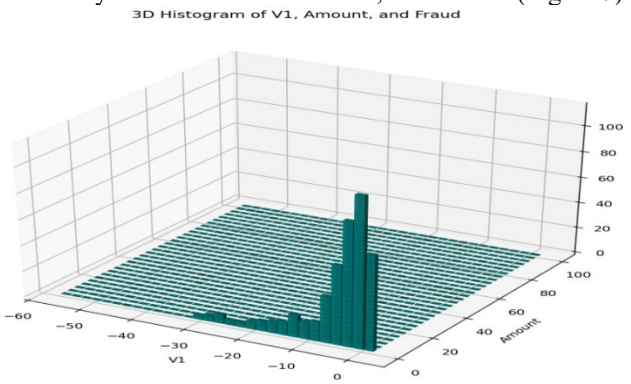

Figure 7. 3D Visualization of Fraud Patterns

Implications for fraud detection the high level of accuracy and model performance metrics indicate that the hybrid CNN-RNN model is a viable solution for credit card fraud detection. Its ability to learn complex patterns from transaction data allows for fraud detection in real-time, which is crucial in preventing financial losses.

DATA Distribution Analysis

The feature distributions for the selected principal components (V1, V2, V3) were analyzed to understand their separability with respect to the class labels. Figures 8–10 display kernel density estimates (KDE) overlaid with histograms for each feature:

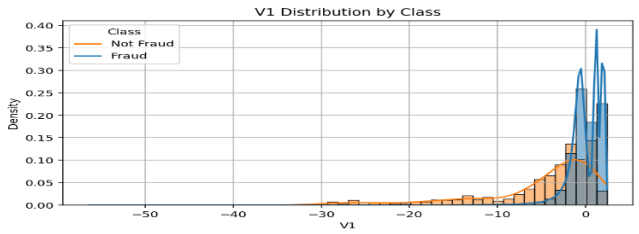

Figure 8. V1 plot

V1 (Figure 8): Fraudulent transactions are sharply concentrated close to zero, while legitimate transactions are more scattered with a left-skewed tail.

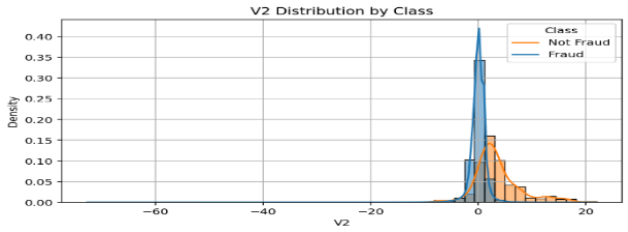

Figure 9. V2 plot

V2 (Figure 9): A similar trend is observed; however, fraudulent cases show a strong peak near the origin, indicating less variation.

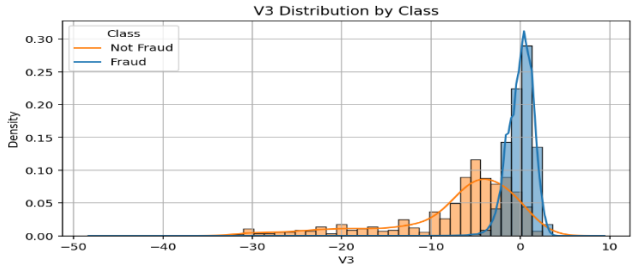

Figure 10. V3 plot

V3 (Figure 10): Presents clear class-based divergence, with fraudulent cases tightly packed between -2 and 2, suggesting discriminative utility.These differences support the hypothesis that some of the latent features from the PCA transformation contain fraud-specific patterns, which the hybrid model can exploit.

Comparison

The high level of accuracy and model performance metrics indicate that the hybrid CNN-RNN model is a viable solution for credit card fraud detection. Its capacity to learn complex designs from exchange information permits fraud detection in real-time, which is significant in avoiding financial misfortunes. Table 4 compares the proposed model's Accurcy against several approaches from related work.

Table 4. Comparative result of accuracy with previous studies

Ref.	Model/Technique	Accuracy
[14]	AEE-GRU	99%
[15]	LSTM + attention	97.5%
[16]	Inception-ResNet-v2)	96.57%
[18]	Machine Learning classification	98.33%
[19]	ANN, RNN, LSTM	95.9%
Our proposed model	**Hybrid CNN-RNN**	**99.72%**

Limitations and Future Work

Whereas the model shows high accuracy, it is fundamental to consider the plausibility of overfitting, particularly in highly imbalanced datasets. Future work can investigate methods such as cross-validation and alternative oversampling strategies to improve the robustness of the model. Furthermore, exploring the interpretability of the model expectations may give assist understanding into the features that contribute to fraud detection.

CONCLUSION

This study proposes a strong hybrid deep learning model combining CNN and RNN for credit card fraud detection in exceedingly imbalanced datasets. By leveraging CNNs capacity to extricate spatial designs and RNNs quality in modeling transient conditions, the model successfully distinguished fraudulent exchanges with high accuracy and negligible false positives. The integration of Destroyed oversampling assist addressed the class awkwardness, expanding the model's sensitivity to uncommon fraud cases. Test comes about illustrated that the hybrid CNN-RNN design accomplished prevalent performance in numerous assessment metrics counting accuracy, precision, recall, F1-score, and AUC. Visualizations such as ROC curves, confusion matrices, and density plots affirmed the discriminative control and joining stability of the model. This study approves the adequacy of combining spatial and successive feature learning in financial fraud detection and gives a practical deep learning system that can be adjusted to other inconsistency detection errands in imbalanced domains.

REFERENCES

Ahmed, S. F., Alam, M. S. B., Hassan, M., Rozbu, M. R., Ishtiak, T., & Rafa, N. (2023). Deep learning modelling techniques: current progress, applications, advantages, and challenges. *Artificial Intelligence Review*, *56*(11), 13521–13617,.

Alzubaidi, L., Zhang, J., Humaidi, A. J., Al-Dujaili, A., Duan, Y., & Al-Shamma, O. (2021). Review of deep learning: concepts, CNN architectures, challenges, applications, future directions. *Journal of Big Data*,

8(1), 53.

Benchaji, I., Douzi, S., Ouahidi, B. E., & Jaafari, J. (2021). Enhanced credit card fraud detection based on attention mechanism and LSTM deep model. *Journal of Big Data*, *8*(1), 151.

Credit Card Fraud DetectionNo Title. (n.d.). https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud

de Jesus Jr, F. F.-N., & Carbonero-Ruz, M. (2025). Enhancing financial time series forecasting through topological data analysis. *Neural Computing and Applications*, *37*(9), 6527–6545,.

Elreedy, D., Atiya, A. F., & Kamalov, F. (2024). A theoretical distribution analysis of synthetic minority oversampling technique (SMOTE) for imbalanced learning. *Machine Learning*, *113*(7), 4903–4923,.

Ibrahim, N., Abbas, A., & Khorsheed, F. (2023). A systematic review for misuses attack detection based on data mining in NFV. *Sakarya University Journal of Computer and Information Sciences*, *6*(3), 239–252,. https://doi.org/10.35377/saucis.1379047.

Ileberi, E., & Sun, Y. (2024). A Hybrid Deep Learning Ensemble Model for Credit Card Fraud Detection. *IEEE Access*.

Janbhasha, S., Kumar, C. S., Sitharamulu, V., Babu, B. M., Battu, H. R., & Venkataramana, K. (2025). A hybrid approach for fraud detection in digital wallet transactions using adversarial autoencoders and gated recurrent units. *Engineering, Technology & Applied Science Research*, *15*(4), 25532–25537,.

Kafhali, S. E., Tayebi, M., & Sulimani, H. (2024). An optimized deep learning approach for detecting fraudulent transactions. *Information*, *15*(4), 227.

Karthika, J., & Senthilselvi, A. (2023). Detection of credit card fraud detection using HPO with inception based deep learning model. *Proc. 2023 5th Int. Conf. Inventive Res. Comput. Appl. (ICIRCA*, 70–77.

Kennedy, R. K., Villanustre, F., Khoshgoftaar, T. M., & Salekshahrezaee, Z. (2024). Synthesizing class labels for highly imbalanced credit card fraud detection data. *Journal of Big Data*, *11*(1), 38.

Mienye, I. D., Swart, T. G., & Obaido, G. (2024). Recurrent neural networks: A comprehensive review of architectures, variants, and applications. *Information*, *15*(9), 517.

Njoku, D. O., Iwuchukwu, V. C., Jibiri, J. E., Ikwuazom, C. T., Ofoegbu, C. I., & Nwokoma, F. O. (2024). Machine learning approach for fraud detection system in financial institution: A web base application. *Machine Learning*, *20*(4), 01–12,.

Ramaiya, V., Goyal, P., & Dubey, N. K. (2024). Cybersecurity Threats and Trust Dynamics in Digital Payment Systems: An Analysis of Domestic Fraud and User Perspectives. *Proc. Int. Conf. on Advancements in Smart Computing and Information Security*, 116–138.

Sharma, S., Kataria, A., Sandhu, J. K., & Ramkumar, K. R. (2022). Credit card fraud detection using machine and deep learning techniques. *Proc. 2022 3rd Int. Conf. for Emerging Technology (INCET*, 1–7.

Udayakumar, R., Joshi, A., Boomiga, S. S., & Sugumar, R. (2023). Deep fraud Net: A deep learning approach for cyber security and financial fraud detection and classification. *Journal of Internet Services and Information Security*, *13*(3), 138–157,.

Wiese, B., & Omlin, C. (2009). Credit card transactions, fraud detection, and machine learning: Modelling time with LSTM recurrent neural networks. In *Innovations in Neural Information Paradigms and Applications* (pp. 231–268). Springer.

Yoganandham, G., & Elanchezhian, G. (2024). Analyzing the Economic Impact of Credit Card Fraud: Activation, Limit Upgrades, Cashback Scams, Discount Fraud, and Overdraft Risks. *Degrés*, *9*(11).

ConflictofInterestStatement: Theauthorsdeclarethattheresearchwasconducted in the absence of any commercial or financial relationships that could be construed as a potential conflict ofinterest.