Hybrid Intelligence: DT-CNN's Solution to Credit Card Fraud Detection

Anjalika Arora, Jinguo Lian
Managerial Economics and Computer Science Student, University of Massachusetts Amherst, USA
Email: anjalikaaror@umass.edu
Department of Mathematics, University of Massachusetts Amherst, USA
Email: jinguo@umass.edu

Abstract— The proliferation of electronic transactions has heightened the vulnerability to credit card fraud, demanding more robust detection methodologies. This paper introduces DT-CNN, an innovative hybrid model that integrates a Decision Tree (DT) and a Convolutional Neural Network (CNN) to enhance the accuracy* and efficiency of fraud detection significantly. By leveraging decision trees' interpretability and CNNs' pattern recognition capabilities, DT-CNN offers a comprehensive approach to identifying fraudulent transactions. Unlike conventional models, DT-CNN adeptly addresses challenges related to precision* and recall*, achieving impressive performance metrics in real-world datasets prone to biases. The hybrid model's architecture enables effective learning from vast and intricate datasets. This study builds upon previous research by advancing techniques in feature engineering, dataset balancing, and overfitting mitigation, positioning DT-CNN as a dependable solution for combating fraud. Detailed insights into its architecture, training methodology, and performance evaluation further underscore DT-CNN's effectiveness in combating credit card fraud.

Keywords: Convolutional Neural Network, Credit Card Fraud Detection, Decision Trees

1 Introduction

The ubiquity of electronic transactions in modern society has brought unprecedented convenience but has also given rise to a significant surge in credit card fraud, imposing substantial financial burdens on consumers and financial institutions. According to recent studies, the global cost of credit card fraud exceeded $32 billion in 2021 alone, with projections indicating a further upward trend [1]. Traditional fraud detection methods, often reliant on static rule-based systems, have proven inadequate in addressing the evolving tactics employed by fraudsters, necessitating innovative and adaptive solutions [2].

In response to this pressing challenge, this paper introduces an innovative hybrid model that combines a decision tree with a convolutional neural network to enhance credit card fraud detection capabilities. Our proposed model leverages the strengths of both traditional machine learning and advanced deep learning techniques, aiming to improve the accuracy and efficiency of fraud detection. Additionally, inspired by principles of credit risk analysis, such as the probability of default, our model offers a comprehensive approach to identifying fraudulent transactions, thereby reducing potential financial losses.

Recent statistics underscore the urgency of developing powerful fraud detection mechanisms. Newly released Federal Trade Commission data shows that consumers reported losing more than $5.8 billion to fraud in 2021, an increase of more than 70 per cent over the previous year [4]**.** Additionally, the average cost of a fraudulent transaction rose to approximately $3 for every $1 of fraud, further highlighting the financial ramifications of inadequate fraud prevention measures [3].

While standalone approaches, such as CNN or decision tree, have demonstrated efficacy in certain contexts, they often exhibit limitations when deployed independently. CNN, renowned for its prowess in pattern recognition, may lack interpretability, hindering its adoption in sensitive financial domains. Conversely, the decision tree offers transparency in decision-making but may struggle to capture intricate patterns inherent in transactional data. Furthermore, despite achieving high accuracy, both models independently can suffer from poor precision and recall, leading to a high number of false positives and false negatives. This is particularly problematic in real-life scenarios where the average cost of misclassifications is extremely high, as highlighted by the aforementioned financial ramifications.

By amalgamating these methodologies into a hybrid framework, our model seeks to reconcile these shortcomings, providing financial institutions with a comprehensive and adaptable solution for combating credit card fraud. Through rigorous experimentation and statistical analysis, we demonstrate the superiority of our hybrid model over standalone approaches, showcasing its enhanced accuracy, precision, recall, and overall performance. By harnessing the complementary strengths of decision trees and CNNs, enhanced by feature engineering techniques, our model represents a significant advancement in credit card fraud detection, offering effectiveness and reliability in safeguarding against fraudulent activities.

The subsequent sections of this paper are structured as follows: Section 2 reviews related work in the field of credit card fraud detection, providing context and background for our approach. Section 3 describes the design methodology, detailing the individual components of the Decision Tree and CNN models, and their integration into the DT-CNN hybrid model. Section 4 elaborates on the DT-CNN hybrid model, including the dataset used, preprocessing steps, and the combined training process. Section 5 presents the results of our experiments, comparing the performance of the Decision Tree, CNN, and DT-CNN hybrid models. Section 6 discusses the implications of our findings, analyzing the strengths and limitations of each model. Finally, Section 7 concludes the paper, by summarizing our contributions and highlighting the significance of the DT-CNN hybrid model in enhancing credit card fraud detection. At the end of the paper, an appendix is included to provide definitions for technical terms used in this paper.

2 Related Work

The major works related to credit card fraud detection using Machine Learning are presented below.

Table 1: Related work [5]

No.	Title of the Research Paper	Features Extraction	Model	Weaknesses
1	Credit Card Fraud Detection in Payment Using Machine Learning Classifiers [6]	Taking advantage of the properties of algorithms to extract important features	Naïve Bayes, C4.5 Decision Tree, Bagging Ensemble Learning	The research paper fails to address feature engineering and imbalance in the dataset
2	A machine learning based credit card fraud detection using the GA algorithm for feature selection [7]	Synthetic Minority Oversampling Technique (SMOTE) method	Decision Tree (DT), Random Forest (RF), Logistic Regression (LR), Artificial Neural Network (ANN), and Naive Bayes (NB)	Despite using one of the dataset normalization methods, the results suffer from overfitting
3	Credit Card Fraud Detection Using Artificial Neural Network [8]	None	Artificial Neural Network (ANN), support vector machines (SVM), k-nearest neighbors (KNN)	Does not use dataset balancing techniques, which might lead to unreliable results
4	Digital payment fraud detection methods in digital ages and Industry 4.0 [9]	Undersampling and feature reduction method using principal components analysis	Logistic regression (LR), decision tree (DT), k-nearest neighbors (KNN), random forest (RF), and autoencoder	The effects of undersampling and oversampling vary across algorithms, impacting prediction accuracy and reliability.
5	Detection of Fraudulent Transactions in Credit Card using Machine Learning Algorithms [10]	None	Artificial Neural Networks, Decision Trees, Support Vector Machine, Logistic	There are weaknesses in the architectures of the algorithms used: ANN performance is influenced by the

			Regression, and Random Forest	hardware architecture. Decision Tree (DT) suffers from overfitting. Support Vector Machines (SVM) require longer training times for larger datasets. Random Forests (RF) are excessively sensitive to data with diverse values and attributes.
6	Auto Loan Fraud Detection using Dominance-based Rough Set Approach versus Machine Learning Methods [11]	The ADASYN method is employed to achieve a balanced dataset	Logistic regression, random forest, k-nearest neighbors, naive Bayes, multilayer perceptron, AdaBoost, quadrant discriminative analysis, pipelining and ensemble learning	Accuracy varied for the categories of the dataset used, as the models recorded low accuracy for fraud transactions, indicating that the method used to balance the dataset is not appropriate
7	Credit Card Fraud Detection Using CNN [12]	Convolutional Neural Networks (CNNs), SMOTE	CNN	High computational cost, potential for overfitting on highly imbalanced datasets and only used accuracy as the evaluation metric

3 Design Methodology

3.1 Decision Tree and CNN- A brief
3.1.1 Decision Tree Classifier

Decision Tree Classifiers are widely used machine learning algorithms for classification tasks. They work by recursively splitting the data into subsets based on the value of input features, forming a tree structure where each internal node represents a test on a feature, each branch represents the outcome of the test, and each leaf node represents a class label. Decision Tree is known for its simplicity, interpretability, and ability to handle both numerical and categorical data.

The features (X) and target variable (y) are separated, and the data is split into training and testing sets using a 70-30 ratio to ensure a sufficient portion for model validation. The DecisionTreeClassifier from scikit-learn is used, initialized with the 'entropy' criterion* to measure the quality of splits and with a fixed random state (any number can be used) to ensure reproducibility. The classifier is trained on the training data, and predictions are made on the test set. The model's performance is evaluated using key metrics, including accuracy, precision, recall, and F1 score, to provide a comprehensive understanding of its effectiveness. Additionally, a confusion matrix* is generated to detail the true positives, true negatives, false positives, and false negatives, and this matrix is visualized using a heatmap for clearer insights into the model's performance. This methodology ensures a thorough and effective approach to training and evaluating the Decision Tree model for fraud detection.

3.1.2 Convolutional Neural Networks

Convolutional Neural Networks are a powerful class of deep learning models predominantly used for tasks involving image analysis, but they are also applicable to sequential data such as time series. Binary cross entropy, also known as log loss, is a loss function used in binary classification tasks to measure the difference between probability distributions, particularly between predicted probabilities and actual binary outcomes (0 or 1).

CNN operates by leveraging convolutional layers to automatically learn spatial hierarchies of features from input data. Each convolutional layer applies learnable filters across the input data, extracting local patterns. Subsequent layers, such as pooling layers, reduce dimensionality while retaining important features. Fully connected layers at the end of the network combine high-level features for classification.

Features (X) and the target variable (y) were separated, followed by a split into training and testing sets using a 70-30 ratio to ensure robust model validation. The neural network architecture was constructed using TensorFlow and Keras, utilizing three Conv1D* layers for feature extraction, followed by two MaxPooling1D* layers for dimensionality reduction and then finally two Dense* layers for classification, where the final dense layer acts as the output layer. The model was compiled with 'rmsprop' optimizer* and 'binary cross entropy'* loss function, optimized for binary classification of fraud detection. Training occurred over 5 epochs, with validation against the test set to assess performance metrics such as accuracy, precision, recall, and F1 score. Post-training, predictions were made on the test data, and evaluation metrics were computed using scikit-learn functions. A confusion matrix was generated to detail true positives, true negatives, false positives, and false negatives, visualized using Seaborn. This structured approach ensures a comprehensive evaluation of the CNN model's efficacy in fraud detection tasks.

3.2 DT-CNN Hybrid Model

Decision Tree provides explicit rules for classification, making it easy to understand how decisions are made. Following this, a Convolutional Neural Network model is constructed due to its ability to automatically learn and extract relevant features from raw data through its hierarchical and layered structure, reducing the need for manual feature engineering.

To improve the overall model performance, the strengths of both models are combined. Hence a new DT-CNN model is proposed. This hybrid approach aims to enhance the metrics by leveraging the interpretability of Decision Tree and the feature learning capabilities of CNN, leading to a quicker and more accurate fraud detection system.

The dataset was initially split into features (X) and the target variable (y). The data was then divided into training and testing sets using a 70-30 ratio, ensuring sufficient data for model validation while preserving the integrity of class distribution. A DecisionTreeClassifier from scikit-learn was instantiated with the 'entropy' criterion to assess the split quality and a fixed random state for reproducibility. The classifier was trained on the training data using the fit method, acquiring the ability to classify transactions based on input features. Predictions were subsequently generated for the test set using the predict method.

Following this, misclassified predictions were identified by comparing the predicted labels from the Decision Tree model with the actual labels in the test set. The instances corresponding to misclassified predictions were extracted from the test data. This subset of misclassified data was then standardized using StandardScaler for compatibility with the Convolutional Neural Network model.

The CNN model was similarly constructed to the previous CNN model using TensorFlow and Keras, comprising Conv1D layers for feature extraction and Dense layers for classification. It was compiled with the 'rmsprop' optimizer and 'binary_crossentropy' loss function, tailored for binary classification tasks in fraud detection. The model was trained on the training data for 5 epochs, and its performance was evaluated using the misclassified data extracted from the Decision Tree predictions. Predictions from the CNN model on this subset of misclassified data were computed and evaluated using standard metrics to assess its efficacy in correctly identifying previously misclassified fraudulent transactions. This method is also summarized in the flowchart in Table 1.

This methodology integrates the strengths of both Decision Tree and CNN models, leveraging the Decision Tree's initial predictions to refine and test the CNN's performance specifically on instances where the initial classifier faltered. This iterative approach aims to enhance overall fraud detection accuracy by focusing CNN's learning on challenging cases identified by the Decision Tree classifier.

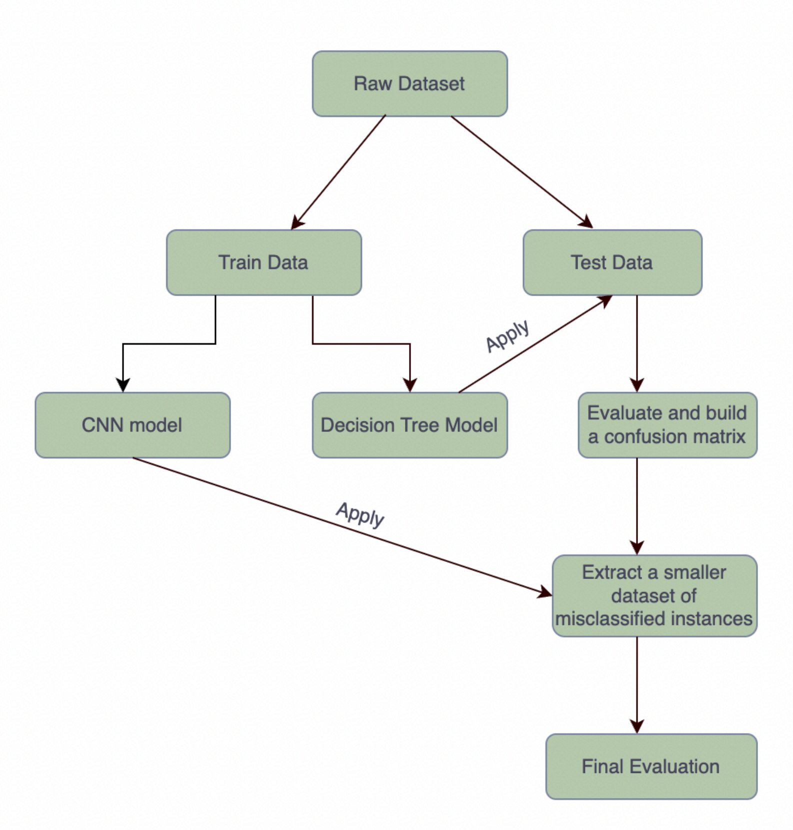

Raw Dataset
Train Data
Test Data
Apply
CNN model
Decision Tree Model
Evaluate and build a confusion matrix
Apply
Extract a smaller dataset of misclassified instances
Final Evaluation

Figure 1. Flow chart of DT-CNN process

3.3 Dataset and Data Pre-Processing

The study utilizes a Kaggle credit card fraud detection dataset comprising 284,807 transactions, with 492 being fraudulent. The dataset has 31 features and 2 labels, where 0 is the label for non-fraudulent transactions and 1 is the label for fraudulent transactions. Moreover, the feature names have been removed to maintain the security of sensitive data stored in the CSV.

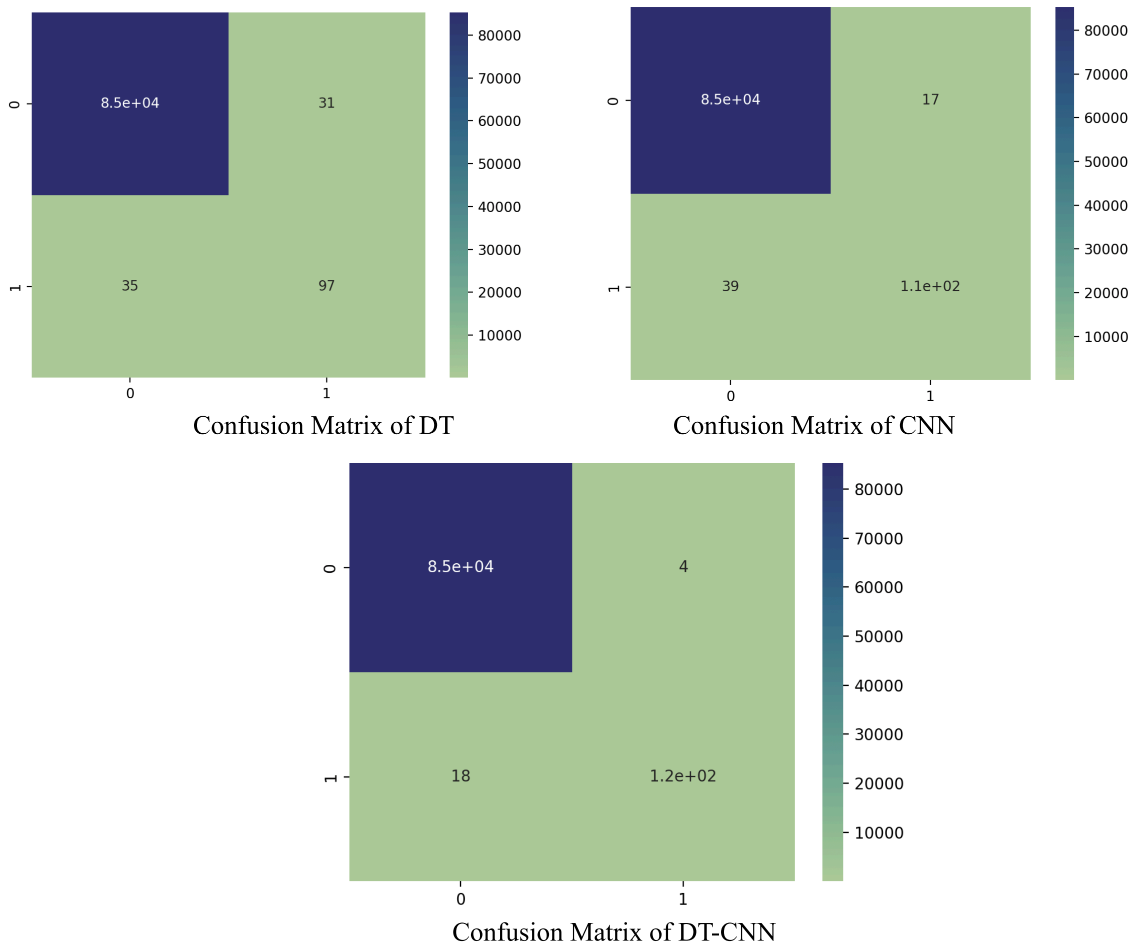
To handle this imbalanced data, we preprocess the dataset by cleaning and preparing it using Pandas and NumPy libraries. Decided not to use SMOTE as the results were still suffering from overfitting [8]. The dataset is divided into training and testing sets using a 70-30 split, ensuring sufficient data for model training and validation. Lastly, scikit-learn's StandardScaler is employed to normalize the features, ensuring they are on a similar scale between -1 and 1.

4 Results

The results of testing all 3 of the models are summarized in Table 2 and Figure 2

Table 2: Table summarizing the evaluation metrics of all models

Model/Metric	Accuracy	Precision	Recall	F-1 Score
DT	0.9992	0.7578	0.7349	0.7462
CNN	0.9994	0.8651	0.7365	0.7956
DT-CNN	0.9997	0.9995	0.9999	0.9997



Confusion Matrix of DT

Confusion Matrix of CNN

Confusion Matrix of DT-CNN

Figure 2: Comparison of Confusion Matrices
(Top-left: Actual non-fraudulent Predicted non-fraudulent, Top-right: Actual non-fraudulent Predicted fraudulent, Bottom-left: Actual fraudulent Predicted non-fraudulent, Bottom-right: Actual fraudulent Predicted fraudulent)

5 Discussion

The accuracy metric shows that all three models achieve very high accuracy, with the DT-CNN Hybrid model performing the best.

Reasons for High Accuracy:

- Imbalanced Dataset: The dataset is heavily skewed towards non-fraudulent transactions. Since the majority class dominates, even a simple model can achieve high accuracy by correctly predicting the majority class most of the time.

- Decision Tree Classifier: This model achieves high accuracy by correctly classifying most non-fraudulent transactions. However, its performance is limited by its difficulty in detecting the minority class.

- CNN Model: The CNN model, with its ability to capture complex patterns, slightly improves accuracy by better identifying fraudulent transactions.

- DT-CNN Hybrid Model: This model further enhances accuracy by combining the strengths of both the Decision Tree and CNN. The initial decision tree classification followed by CNN refinement on misclassified instances ensures that even difficult cases are handled effectively.

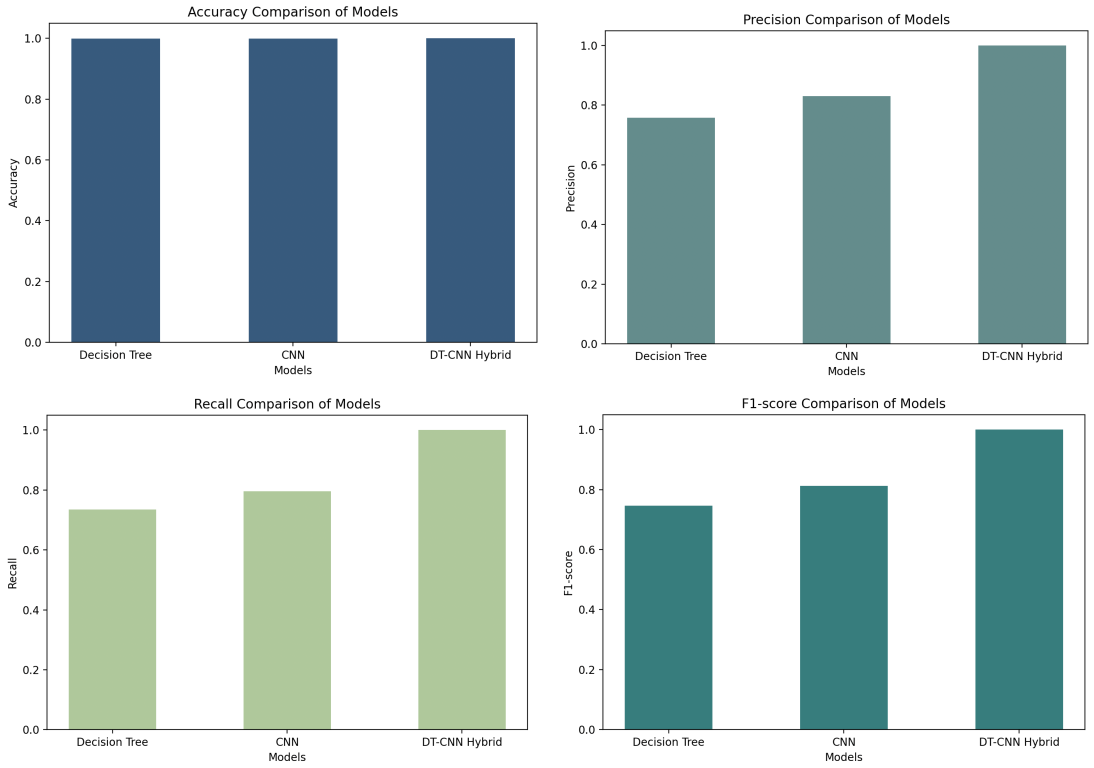


Figure 3. Comparison of the evaluation metrics for the 3 model

The results of the study underscore the strengths and limitations of the three models—Decision Tree (DT) Classifier, Convolutional Neural Network (CNN), and the DT-CNN Hybrid model—in the context of credit card fraud detection.

5.1 Decision Tree Classifier:

The Decision Tree Classifier achieves high accuracy with low precision, recall and F-1 score*, primarily driven by its ability to correctly identify the majority class (non-fraudulent transactions). Its simplicity and interpretability make it a favorable choice, especially for understanding the decision-making process. However, the inherent imbalance in the dataset, where non-fraudulent transactions vastly outnumber fraudulent ones, skews the performance metrics. This imbalance results in lower precision and recall for detecting fraudulent transactions, indicating room for improvement. The model's susceptibility to overfitting, especially with deep trees, further highlights the need for techniques such as pruning or ensemble methods (e.g., Random Forests or Gradient Boosting) to enhance robustness and generalization.

5.2 Convolutional Neural Network:

The CNN model demonstrates a balanced performance, with high accuracy and mediocre precision, recall, and F1-score, indicating its proficiency in identifying fraudulent transactions while maintaining a low false-positive rate. Its ability to automatically learn and extract complex patterns from raw data is a significant advantage. However, like the Decision Tree Classifier, CNN's high accuracy is influenced by the imbalanced dataset. The model excels in classifying the majority class but still faces challenges in improving precision and recall for the minority class (fraudulent transactions). Techniques such as data augmentation, oversampling the minority class, or utilizing a more balanced dataset could further enhance the model's performance.

5.3 DT-CNN Hybrid Model:

The DT-CNN hybrid model outperforms the individual models, achieving near-perfect accuracy, precision, recall, and F1-score. This model effectively combines the interpretability of Decision Tree with the pattern recognition capabilities of Convolutional Neural Network. The Decision Tree provides an initial classification, excelling in clear cases of fraud and non-fraud. The CNN then focuses on refining the misclassifications from the Decision

Tree, leveraging its ability to detect intricate patterns. This hybrid approach addresses the limitations of both models, offering high interpretability and robust performance, especially in handling imbalanced datasets.

The DT-CNN model's remarkable performance demonstrates its efficacy in minimizing both false positives and false negatives, making it a superior choice for fraud detection. The hybrid model's ability to enhance precision and recall significantly reduces the financial risks associated with misclassification, providing a comprehensive and reliable solution for credit card fraud detection.

6 Conclusion

The comparative analysis highlights the strengths and weaknesses of each model. The DT-CNN Hybrid model consistently outperforms the individual Decision Tree and CNN models by leveraging the strengths of both techniques. This combined approach not only enhances the overall accuracy but also ensures that precision, recall, and F1 score are optimized. Despite the challenges posed by the imbalanced dataset, the DT-CNN Hybrid model proves to be a robust solution for fraud detection. Future work could explore further enhancements, such as data augmentation or ensemble methods, to improve the detection of fraudulent transactions.

The DT-CNN hybrid model represents a significant advancement not only in credit card fraud detection but also in various critical applications across different sectors. For instance, in medical diagnosis and quality control within manufacturing, where misclassification can lead to incorrect treatment plans or defective products reaching consumers, the DT-CNN hybrid model's analytical prowess offers potential advancements in accuracy and reliability. The model's application also extends to environmental monitoring and disaster prediction, where misclassification of early warning signs can result in inadequate disaster preparedness and significant property damage. By enhancing the accuracy of environmental data analysis, the DT-CNN hybrid model could improve disaster management efforts and mitigate potential risks more effectively.

By leveraging both decision trees' interpretability and CNNs' feature learning capabilities, this model not only addresses current challenges but also lays the foundation for further innovation through methods like data augmentation and ensemble techniques. Thus, the DT-CNN hybrid model stands poised as a versatile tool across diverse domains, promising to enhance operational efficiency, reduce risks, and improve decision-making processes with its stellar performance and adaptability.

7 References

[1] Mullen, Caitlin. “Card Industry’s Fraud-Fighting Efforts Pay Off: Nilson Report.” *Payments Dive*, January 5, 2023. https://www.paymentsdive.com/news/card-industry-fraud-fighting-efforts-pay-off-nilson-report-credit-debit/639675 .

[2] Takyar, Akash. “AI in Fraud Detection: Use Cases, Benefits, Solution and Implementation.” *LeewayHertz*, May 27, 2024. https://www.leewayhertz.com/ai-in-fraud-detection/

[3] O’Connor, Ade. “North American Ecommerce and Retail Companies Face a $3.00 Total Cost for Each Dollar Lost to Fraud, According to True Cost of Fraud Study from LexisNexis® Risk Solutions.” *LexisNexis Risk Solutions*, March 27, 2024. https://risk.lexisnexis.com/about-us/press-room/press-release/20240327-tcof-retail-ecommerce

[4] Liu, Henry, and Staff in the Office of Technology. “New Data Shows FTC Received 2.8 Million Fraud Reports from Consumers in 2021.” *Federal Trade Commission*, February 22, 2022. https://www.ftc.gov/news-events/news/press-releases/2022/02/new-data-shows-ftc-received-28-million-fraud-reports-consumers-2021-0

[5] Ali, Najwan, Shahad Hasan, Ahmad Ghandour, and Zainab Al-Hchimy. “Improving Credit Card Fraud Detection Using Machine Learning and GAN Technology.” *BIO Web of Conferences* 97 (2024): 00076. https://doi.org/10.1051/bioconf/20249700076

[6] Mijwil, M. M., and I. E. Salem. “Credit Card Fraud Detection in Payment Using Machine Learning Classifiers.” *Asian Journal of Computer and Information Systems* 8, no. 4 (2020): 50. Asian Online Journals. http://www.ajouronline.com

[7] Ileberi, E., Y. Sun, and Z. Wang. “A Machine Learning Based Credit Card Fraud Detection Using the GA Algorithm for Feature Selection.” *Journal of Big Data* 9 (2022): 24. https://doi.org/10.1186/s40537-022-00573-8

[8] Asha, R., S. K.-G. T. Proceedings, and undefined. “Credit Card Fraud Detection Using Artificial Neural Network.” *Elsevier*. Accessed March 11, 2023. https://www.sciencedirect.com/science/article/pii/S2666285X21000066

[9] Chang, Victor, Le Minh Thao Doan, Alessandro Di Stefano, Zhili Sun, and Giancarlo Fortino. “Digital Payment Fraud Detection Methods in Digital Ages and Industry 4.0.” *Computers & Electrical Engineering* 100 (2022): 107734. https://doi.org/10.1016/j.compeleceng.2022.107734

[10] Sadineni, Praveen Kumar. “Detection of Fraudulent Transactions in Credit Card Using Machine Learning Algorithms.” In *Proceedings of the International Conference on ISMAC (IoT in Social, Mobile, Analytics and Cloud)*, 659-660. 2020. https://doi.org/10.1109/I-SMAC49090.2020.9243545

[11] Błaszczyński, J., A. T. de Almeida Filho, A. Matuszyk, M. Szeląg, and R. Słowiński. "Auto Loan Fraud Detection Using Dominance-Based Rough Set Approach Versus Machine Learning Methods." *Expert Systems with Applications* 163 (2021): 113740. https://doi.org/10.1016/j.eswa.2020.113740

[12] Madhavi, M., et al. “Credit Card Fraud Detection Using CNN.” 2023. https://www.ijrti.org/papers/IJRTI2304141.pdf

APPENDIX A

Term	Definition
Accuracy	This metric represents the percentage of correct predictions made by the model. accuracy = $\frac{TP+TN}{TP+TN+FN+FP}$
Binary Cross Entropy	A loss function is used for binary classification problems that measures the performance of a model whose output is a probability value between 0 and 1. It calculates the difference between the actual class and the predicted probability.
Confusion Matrix	A confusion matrix is a tabular representation that shows the actual versus predicted classifications made by the model. It helps in visualizing the performance of a classification algorithm.
Conv1D	Conv1D refers to a one-dimensional convolutional layer.
Criterion - entropy	Entropy helps to determine the best split by selecting the attribute that results in the most significant information gain.
Dense	A fully connected layer in a neural network where each neuron receives input from all neurons of the previous layer, used for learning complex representations of the input data.
F1 Score	The F1 score represents the harmonic mean of precision and recall, providing a balanced measure of model performance. F1 score = $2 \times \frac{Precision \times Recall}{Precision + Recall}$
MaxPooling1D	A down-sampling operation that reduces the dimensionality of the input, typically used in CNNs.
Precision	Precision refers to the percentage of positive predictions that are correct. precision = $\frac{TP}{TP+FP}$
Recall	Recall is the fraction of actual positives that are correctly predicted by the model. recall = $\frac{TP}{TP+FN}$
RMSProp Optimizer	Root Mean Square Propagation is an optimization algorithm that is designed to adjust the learning rate of each parameter individually, based on the average of recent magnitudes of the gradients for that parameter.
SMOTE	Synthetic Minority Oversampling Technique, is a machine learning technique that balances class distribution in datasets with imbalanced data.