Novel Approaches in Financial Fraud Detection:

Hybrid Machine Learning and Uncertainty-Based Deep Learning

Hadi Mohammadi[1], Mahdieh Rahmati[2], Tina Shahedi[1]

[1]Utrecht University [2]University of Luxembourg

Summary

Goal

To improve fraud detection in the financial sector by addressing challenges like data imbalance and uncertainty.

Motivation

Preventing fraud is essential to minimize losses and maintain consumer trust in financial services.

Applications

The methods aim to enhance fraud detection systems in e-commerce and financial applications.

Key Contributions

•A hybrid pipeline that combines supervised and unsupervised learning to improve performance against data imbalance.
•A deep learning model that incorporates uncertainty management for more robust detection in real-world scenarios.

Findings

The new deep learning approach outperforms traditional models, demonstrating improved accuracy and reliability by effectively addressing data imbalance and uncertainty in fraud detection.

Methods

1. Data Preprocessing

- EDA visualizes and cleans the dataset,
- Outlier detection improves data quality,
- PCA reduces dimensionality with standardization,
- Oversampling balances class proportions (eliminating undersampling).

2. Hybrid Model

- The proposed hybrid model uses K-means clustering to group transactions and identify patterns, aiding in the differentiation between legitimate and fraudulent transactions.
- These clusters are then classified with a deep learning model to enhance detection efficiency.

3. Uncertainty Quantification

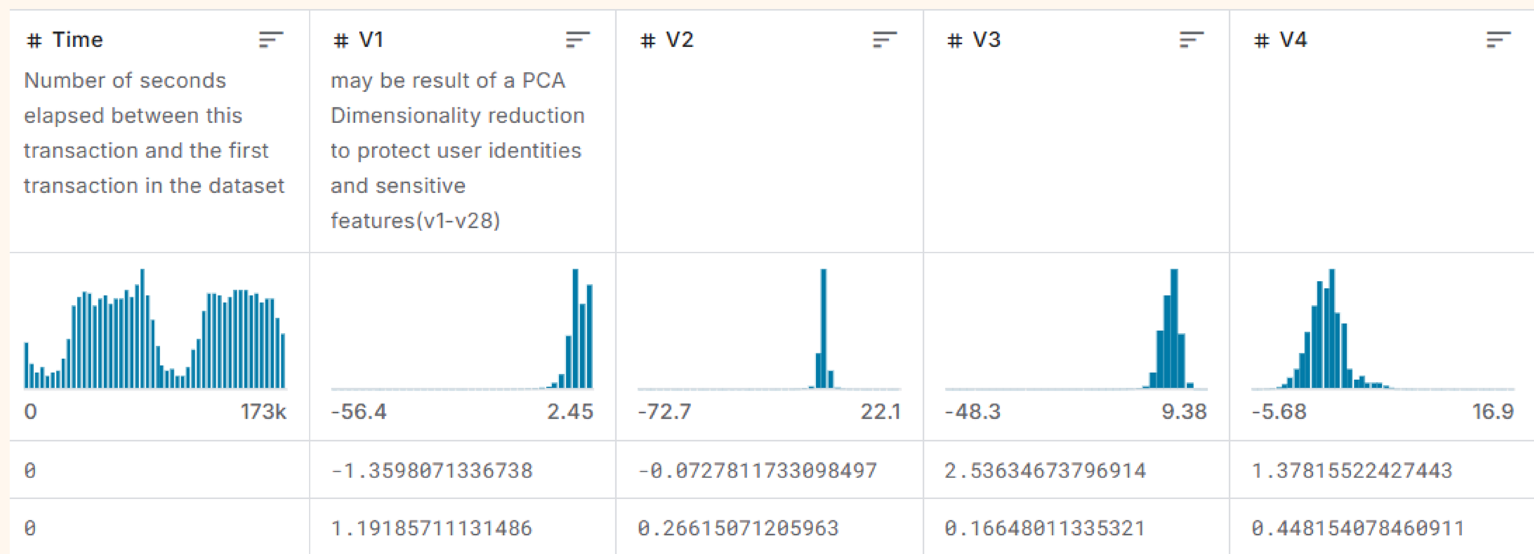
- Utilization of Monte Carlo Dropout (MCD): The model employs MCD to estimate uncertainty and enhance reliability in deep learning.
- Dropout Application: Dropout is used during both training and testing to generate multiple predictions.
- Uncertainty Assessment: These predictions allow for assessing uncertainty in the model's outputs.
- Classification Threshold: A threshold of 0.8 ensures that only high-confidence predictions are considered for high-risk transactions.

4. Model Architecture

- The hybrid model includes a 30-unit input layer, multiple hidden layers with dropout techniques for better learning, and a single-output layer with sigmoid activation for binary classification.

Dataset

The study utilizes the Credit Card Fraud Detection dataset, consisting of **284,807** anonymized transactions from European cardholders, with 492 classified as non-legitimate. It features 30 attributes, including **"Time"** and **"Amount“**, with **V1 to V28** transformed using Principal Component Analysis (PCA) for privacy.

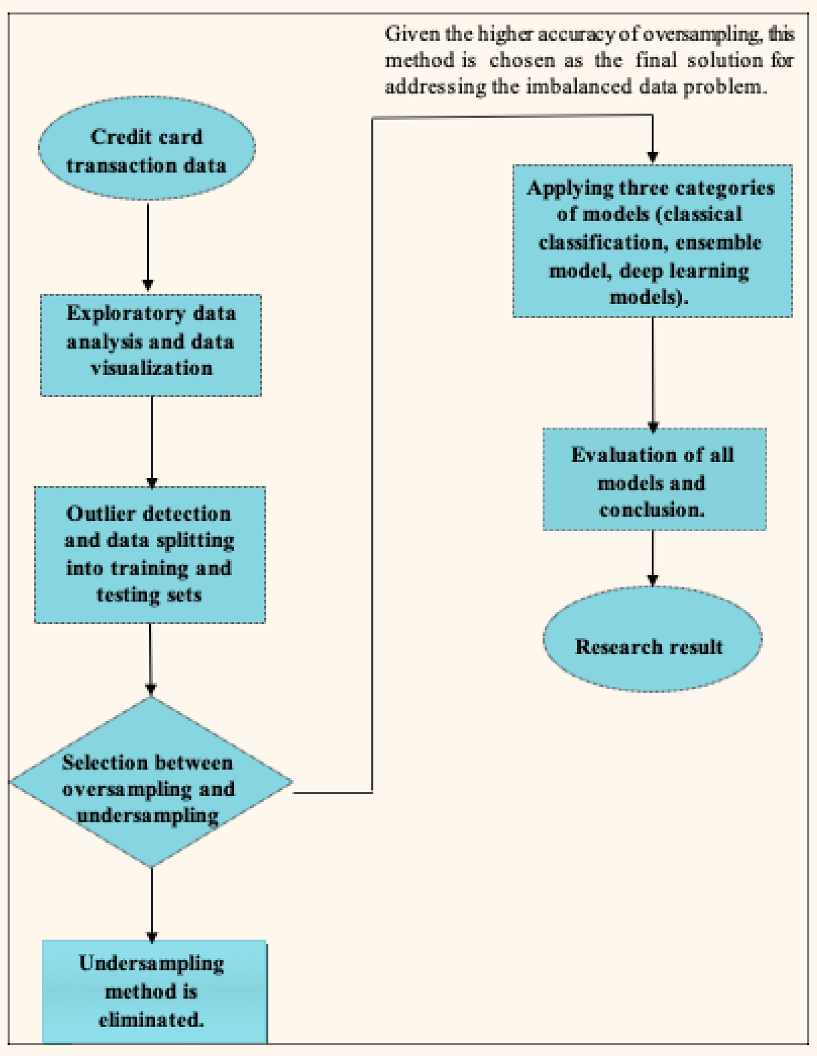


Discussion and Conclusion

The analysis revealed that oversampling outperformed undersampling in addressing data imbalance, and the hybrid deep learning model achieved impressive metrics with an **F1-score** of **0.9990**, compared to **0.9976** for the basic model, although both struggled with minimizing false alarms. Additionally, the hybrid model's use of Monte Carlo Dropout for uncertainty quantification provided valuable insights for prioritizing manual reviews of uncertain transactions, ultimately aiding financial institutions in effectively allocating resources to mitigate the risk of overlooking genuine fraud cases.

Algorithm	TN	FN	TP	FP
Hybrid DL	5485	11	4504	0
Basic DL	4871	23	5106	0
Random Forest with oversampling	14486	418	14517	491

Metric	Hybrid DL	Basic DL	Random Forest
Precision	0.9980	0.9953	0.9637
Recall	1.0	1.0	0.9720
F1-Score	0.9990	0.9976	0.9696
Accuracy	0.9989	0.9977	0.9696



Universiteit Utrecht

UNIVERSITÄT LUXEMBURG