DOI: https://doi.org/10.36094/sc.v92.2026.An_Intelligent_Machine_Learning_Framework.Rana_Akhtar.593

ARTICLE

Sci. and Cult. 92 (9–10) : 593-598 (2026)

AN INTELLIGENT MACHINE LEARNING FRAMEWORK FOR REAL-WORLD DIGITAL TRANSACTION FRAUD DETECTION

ANURAG RANA[1]* AND NAEEM AKHTAR[1]

The study focuses on the increasing significance of digital/e-commerce transaction systems and the associated challenges in the financial services industry today, including the growing incidence of fraudulent activities. We developed a cutting-edge machine learning method to identify frauds in actual digital/e-commerce transactions using a pre-processed version of the IEEE-CIS Fraud Detection dataset. Some of the steps of the process are data cleaning, stratified train-validation-test set split, missing value imputation, feature engineering, feature transformation, categorical feature encoding, model selection, performance tuning with validation set and threshold tuning, and final testing performance analysis. The five machine learning methods studied were logistic regression, random forest, extra trees, XGBoost, and LightGBM. Accuracy will be used together with precision, recall, F1-score, ROC-AUC, and PR-AUC to evaluate the high class imbalance of the dataset. Results of our experiment showed that LightGBM performed better than others. Tweaking the threshold to 0.78, the LightGBM model resulted in an accuracy of 0.9807, a precision of 0.7652, a recall of 0.6406, an F1-score of 0.6974, an ROC-AUC of 0.9560, and a PR-AUC of 0.7430 on the original test set.