

## Abstract

Protection of clients from fraudulent transactions is a complicated task. Banks tend to rely on rule-based systems which require manual creation of rules to identify fraud. These rules have to be set up by employees of the bank who need to look for any trends in fraudulent transactions themselves. This thesis deals with the problem of detection of fraudulent card transactions as it compares multiple machine learning models for fraud detection. These models can find complex relationships in the data and potentially outperform standard fraud detection systems, Logistic regression, neural network, random forest, and extreme gradient boosting (XGBoost) models are trained on a simulated dataset that closely follows properties of real card transactions. Performance of the models is measured by sensitivity, specificity, precision, AUC, and time to predict on the testing dataset. XGBoost shows the highest performance among the tested models. It is then compared to a standard fraud detection system used in a Czech bank. The bank system achieves higher specificity but XGBoost still shows promising performance. It is possible that certain machine learning models could outperform today's fraud detection systems if they are well-tuned.

**JEL Classification** G21, K42  
**Keywords** machine learning, card fraud, fraud detection, imbalanced data  
**Title** Machine Learning Methods in Payment Card Fraud Detection