

Detecting Fraudulent Financial Behavior Through Credit Card Default Patterns: A Machine Learning Approach

Syeda Areeba

Student, Department of Business Administration, University of Sharjah, Sharjah, UAE

Samar Mouakket

Department of Business Information Systems, University of Sharjah, Sharjah, UAE

Abstract:

This study investigates the application of machine learning (ML) algorithms for credit card payment fraud detection and default behaviors. With the growing acceptance of the electronic financial systems, fraud has emerged as a top concern, rendering rule-based systems outmoded since they cannot adapt to evolving fraud patterns. To rectify this issue, the research compares supervised models, such as random forests and decision trees, and unsupervised models, such as clustering and anomaly detection. The findings reveal that supervised approaches are highly effective at predicting fraud based on transactional behavior and that unsupervised approaches detect anomalies without knowing fraud labels beforehand. Additionally, the feature importance analysis showed that the best indicators of default risk and possibly fraudulent activity are recent payments, age, credit limit, and repayment patterns. The research findings demonstrate how machine learning approaches can enhance detection accuracy, minimize false positives and negatives, and enable real-time, scalable fraud detection. The versatility of such integration encourages continuous learning of emerging patterns of fraudulent behavior, leading to improved system performance and user confidence. Employing data from credit card transactions, the study provides evidence of the potential for machine learning to reduce financial losses, strengthen fraud detection systems, and support secure digital payment systems.

Keywords:

Fraud detection, machine learning, supervised learning, unsupervised learning, anomaly detection, scalability, financial transactions, credit card fraud.