Detecção de Fraude em Cartão de Crédito

Luis Henrique Turra Ramos

12 de novembro de 2025

Objetivo: Desenvolver um sistema capaz de identificar transações fraudulentas em tempo real com alta precisão, oferecendo aplicabilidade completa da decisão do modelo por meio de valores SHAP. O objetivo principal foi alcançar recall superior a 92% na classe fraude, mantendo falso positivo controlado, e entregar uma interface interativa que permita simular transações e compreender imediatamente os fatores que levaram à aprovação ou ao bloqueio.

Introdução: Fraudes com cartão de crédito geram bilhões de dólares em prejuízo anualmente. A detecção tradicional baseada em regras torna-se ineficaz diante de constante alterações dos dados. Este projeto propõe uma solução baseada em aprendizado de máquina supervisionado com foco em interpretar padrões, permitindo que analistas de risco compreendam o motivo exato de cada alerta.

Metodologia:

Fontes de Dados: https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud

Técnicas de Análise:

- Pré-processamento: RobustScaler aplicado apenas em Time e Amount; demais variáveis já normalizadas por PCA.
- Balanceamento: combinação de undersampling da classe majoritária com oversampling via SMOTE.
- Modelagem: XGBoost com busca bayesiana.
- Validação: Stratified K-Fold com métricas focadas em recall, precision e AUC-PR.
- Explicação: SHAP
- Interface: aplicação web desenvolvida em Streamlit com duas abas principais – Simulador em Tempo Real e Análise Exploratória Completa.

Limitações: O dataset possui desbalanceamento extremo, o que pode superestimar performance em cenários reais menos desbalanceados.

Resultados:

O modelo final alcançou:

- Recall (fraude): 93,4%
- Precision (fraude): 91,2%
- AUC-ROC: 0,983
- AUC-PR: 0,935

Na interface de simulação, o usuário informa valor e horário da transação; o sistema gera automaticamente valores realistas para V1-V2, tabela com top 10 variáveis mais impactantes (colorida por direção) e resumo textual.

A análise exploratória revelou que fraudes se concentram predominantemente entre 0h e 6h, e que V14, V12, V10 e V17 são consistentemente as variáveis de maior importância e correlação com a classe fraude.

Discussão: Os resultados confirmam que XGBoost combinado com SHAP oferece equilíbrio ideal entre performance e boa interpretação em detecção de fraude. O force plot permite identificar rapidamente padrões como V14 muito negativo significando alta probabilidade de fraude, replicando conhecimento de regras de negócio sem codificá-las manualmente. A concentração de fraudes na madrugada reforça a eficácia de políticas de bloqueio temporário nesse horário.

Conclusões: O sistema desenvolvido atende plenamente ao objetivo inicial: detectar fraudes com recall alto e fornecer explicação clara e imediata para cada decisão. A solução encontra-se pronta para integração em pipelines de autorização de transações, com código limpo e interface acessível a usuários não técnicos.