Prasad V. Potluri Siddhartha Institute of Technology

Fraud Detection in Online Payment Systems

Team 9

Lokesh 22501A0547
Shivani 23505A0506
Mrudula 23505A0501
Subhash 22501A0550

Motivation

Fraud detection is crucial in online payment systems to prevent financial losses and protect users from malicious transactions.

The goal is to build a highly accurate fraud detection system that identifies fraudulent activities while minimizing false alarms.

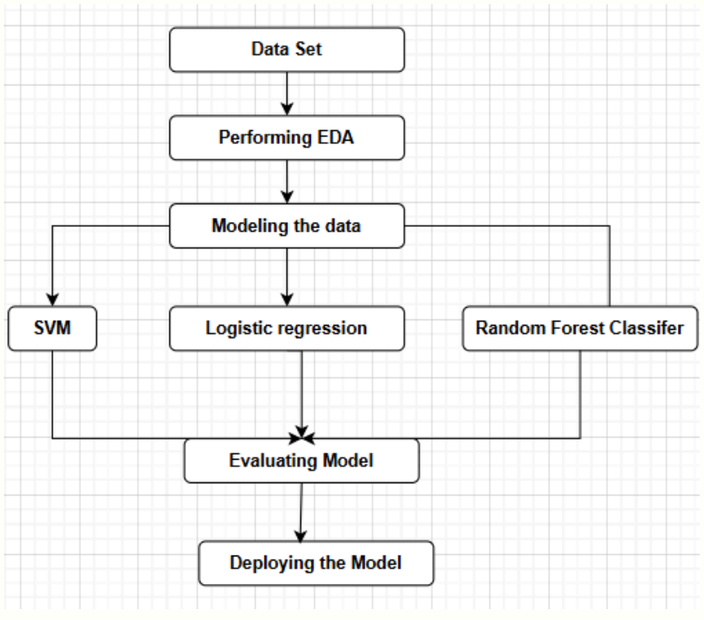
Discussion & Future Work

- **Real-Time Deployment:** Implementing the model as a fraud detection system using APIs.
- **Hybrid Models:** Exploring a combination of decision trees and neural networks for better accuracy.
- **Advanced Techniques**: Investigating deep learning and anomaly detection for improved fraud detection.

Data Collection & Preprocessing

The dataset has 6,362,620 transactions with 11 attributes, including transaction type, amount, and timestamps. It contains 8,213 fraud cases and is preprocessed using feature scaling and balancing for better model performance.

Flow chart



Models

- **Logistic Regression** – Chosen for its simplicity and interpretability in identifying fraud patterns based on transaction attributes.
- **Support Vector Machine (SVM)** – Used for its ability to handle high-dimensional data and detect complex fraud patterns.
- **Random Forest Classifier** – Selected for its robustness, ability to handle imbalanced datasets, and effectiveness in capturing non-linear relationships in fraudulent transactions.

Recomandation Results

- **Best Model & Key Insights:** Random Forest Classifier was the most effective, with most fraud occurring in 'Cash Out' and 'Transfer' transactions, often involving small amounts.
- **Improvements & Future Scope**: Balancing the dataset reduced false positives, and real-time detection with user behavior analysis can further enhance accuracy.