Credit Card Fraud Detection System

Akshat Soni (0827IT221011), Amay Saxena (0827IT221014), Ameer Saif Khan (0827IT221015), Khushi Agrawal (0827IT221076)

Information Technology, Acropolis Institute of Technology & Research, Indore

Session: Jul. – Dec. 2024

Abstract

The Credit Card Fraud Detection system offers an efficient solution to identify and prevent fraudulent transactions in real time. By leveraging machine learning, it ensures high accuracy while minimizing false positives, providing a seamless and secure experience for users. Designed to be scalable and privacy-focused, the system can adapt to various industries, enhancing trust and security in financial transactions.

- **Keywords:** Fraud Detection, Matchine Learning, Data Privacy.

Introduction

The project addresses growing fraud in credit card transactions by developing a robust detection model. It leverages machine learning to analyze transaction patterns, detect anomalies, and prevent unauthorized activities. With a focus on real-time detection, scalability, and privacy preservation, the system ensures security and fosters trust across financial platforms.

Objectives

•**Prevent Fraudulent Transactions**:
Detect and block unauthorized or fraudulent credit card transactions in real-time.

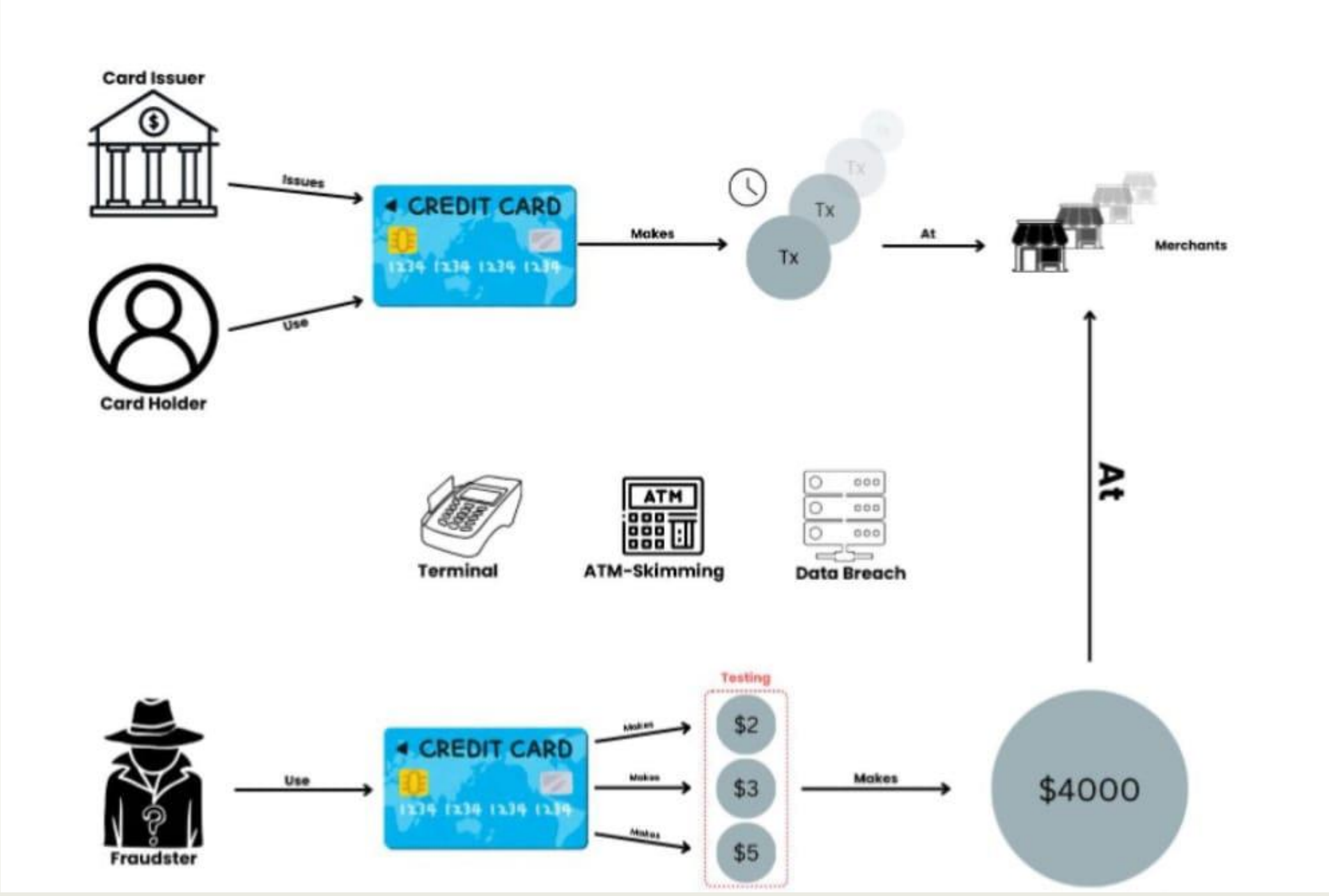
•**Enhance Financial Security**:
Protect users and institutions from financial losses caused by fraud.

•**Reduce False Positives**:
Minimize incorrect flagging of legitimate transactions, ensuring smooth user experiences.

•**Scalable Implementation**:
Create a flexible system that can adapt to various sectors and handle increasing transaction volumes.

•**Preserve Data Privacy**:
Use techniques like dimensionality reduction to ensure user data remains secure and confidential.

Methodology



1. Data Collection:
•Gather past transaction data from financial institutions and public datasets (e.g., Kaggle).
•Ensure diversity in data to cover various types of fraudulent and legitimate transactions.

2. Data Preprocessing:
•Clean the data (handle missing values, outliers, and incorrect entries).
•Normalize numerical features for consistent model training.
•Label the data as fraudulent or legitimate, ensuring accuracy in labels.
•Feature engineering: Extract relevant features such as transaction amount, time, location, etc.

3. Model Implementation:
•Build machine learning models (e.g., CNN, RNN, Random Forest, SVM) for classifying transactions.
•Experiment with deep learning techniques, such as **Convolutional Neural Networks (CNNs)** or **Recurrent Neural Networks (RNNs)**, for better handling of sequential transaction data.
•Evaluate multiple algorithms to choose the best one for the problem.

4. Model Evaluation:
•Split data into training and testing sets.
•Use metrics like accuracy, precision, recall, F1-score, and **AUC-ROC** to evaluate model performance.
•Perform **cross-validation** to ensure model robustness.

Results

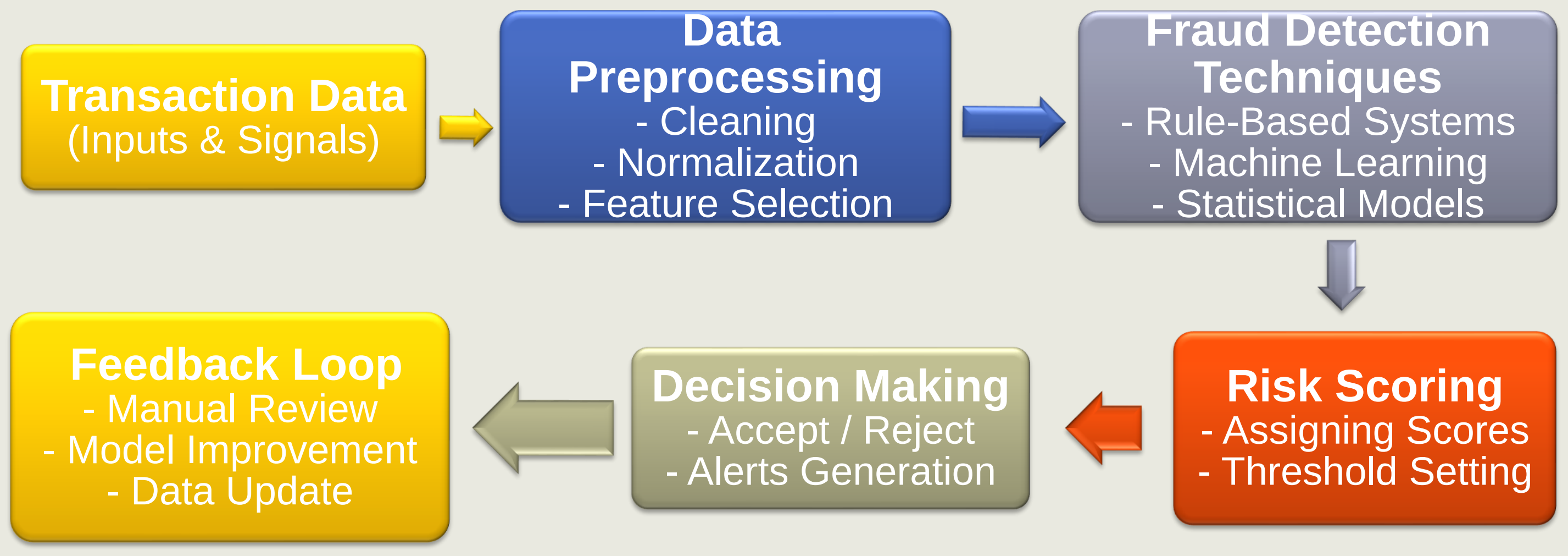
•**Fraud Detection**: Identifies fraudulent transactions from a dataset of credit card transactions.

•**Model Accuracy**: Achieves high accuracy in classifying transactions as fraudulent or legitimate.

•**Data Handling**: Preprocesses data, including scaling and handling imbalances in the dataset.

•**Real-time Application**: Potential for real-time fraud detection in live transaction systems.

•**Evaluation Metrics**: Uses precision, recall, and AUC-ROC to evaluate model performance.



Transaction Data
(Inputs & Signals)

Data Preprocessing
- Cleaning
- Normalization
- Feature Selection

Fraud Detection Techniques
- Rule-Based Systems
- Machine Learning
- Statistical Models

Risk Scoring
- Assigning Scores
- Threshold Setting

Decision Making
- Accept / Reject
- Alerts Generation

Feedback Loop
- Manual Review
- Model Improvement
- Data Update

Conclusion

The **Credit Card Fraud Detection System** provides an efficient real-time solution to identify and prevent fraudulent transactions. By leveraging machine learning, it ensures high accuracy and minimizes false positives, offering a secure and seamless user experience. Scalable and privacy-focused, the system adapts to different industries, continuously learning from new data to detect evolving fraud patterns and enhance trust in financial transactions.

Acknowledgement

- **Project Guide: Prof. (Dr.) Manish Vyas**