AI in Credit Card Fraud Detection

Dr. Pooja Sarin

15 Feb, 2025

1 Introduction

Credit card fraud detection is a crucial application of AI and machine learning (ML). Financial institutions such as **Visa, MasterCard, and PayPal** use AI to analyze transaction history and behavioral patterns to detect anomalies. AI-driven fraud detection aims to identify fraudulent transactions in real-time while minimizing false positives.

2 (a) AI Models for Anomaly Detection in Credit Card Transactions

2.1 Step 1: Data Collection and Preprocessing

AI models require vast amounts of transactional data for training. The collected data includes:

- **Transaction details**: Amount, time, location, and merchant information.
- **User behavior**: Purchase frequency, spending habits, and device usage.
- **Historical fraud data**: Previously detected fraud patterns to improve model learning.

Preprocessing steps include:

- **Feature Engineering**: Extracting relevant features such as transaction velocity and deviation from usual spending behavior.
- **Handling Missing Data**: Filling or removing incomplete transaction records.
- **Data Normalization**: Scaling features for better model performance.

2.2 Step 2: Machine Learning Models Used

Different ML techniques help identify fraudulent transactions:

2.2.1 1. Supervised Learning Models (Labeled Fraud Data)

These models learn from past fraud cases and predict whether a new transaction is fraudulent.

- **Logistic Regression**: Computes probability of fraud based on learned weights:

$$P(Y = 1|X) = \frac{1}{1 + e^{-(\beta_0 + \beta_1 X_1 + ... + \beta_n X_n)}} \quad (1)$$

- **Decision Trees**: Classifies transactions based on decision rules.
- **Random Forests**: Uses multiple decision trees for better fraud prediction.

2.2.2 2. Unsupervised Learning Models (No Labels Required)

These models detect anomalies without labeled fraud cases.

- **Isolation Forests**: Identifies rare anomalies by isolating outliers.
- **Autoencoders**: Neural networks trained to reconstruct transactions. A high reconstruction error signals fraud.
- **Clustering (K-Means)**: Groups similar transactions and flags outliers.

2.2.3 3. Deep Learning Models

- **Recurrent Neural Networks (RNNs)**: Analyze sequential transaction behavior.
- **Graph Neural Networks (GNNs)**: Detect fraud rings using interconnected account behaviors.

2.3 Step 3: Real-Time Detection and Risk Scoring

To detect fraud in real-time, AI systems assign a **risk score** to each transaction:

$$RiskScore = f(\text{Transaction Amount}, \text{Velocity}, \text{Location}, \text{User History}) \quad (2)$$

If the score exceeds a threshold, the transaction is flagged for manual review.

3 (b) Challenges in AI-Based Fraud Detection

3.1 Challenge 1: Handling False Positives

- False positives occur when legitimate transactions are incorrectly flagged as fraud.
- This can lead to customer dissatisfaction and loss of trust.
- **Solution:** Adaptive AI models adjust fraud thresholds based on user behavior.

3.2 Challenge 2: Adaptive Fraud Techniques

- Fraudsters continuously evolve techniques to bypass detection.
- AI models must be updated regularly to recognize new fraud patterns.
- **Solution:** Online learning models that update in real-time.

3.3 Challenge 3: Scalability and Processing Time

- Financial institutions process **millions of transactions per second**.
- AI models must balance accuracy with computational efficiency.
- **Solution:** Use of **cloud-based distributed AI systems**.

3.4 Challenge 4: Balancing Fraud Detection and Customer Experience

- Overly strict fraud detection may block legitimate transactions.
- Users may face inconvenience due to transaction rejections.
- **Solution:** Use **behavioral biometrics and multi-factor authentication** (e.g., OTP verification).

4 Conclusion

AI-driven fraud detection is essential for secure financial transactions. By combining **supervised learning, unsupervised learning, and deep learning**, financial institutions can effectively identify fraudulent activities while minimizing false positives. However, continuous updates and ethical considerations are necessary for long-term success.