GUARDING TRANSACTIONS WITH AI-POWERED CREDIT CARD FRAUD DETECTION AND PREVENTION

Student Name: Srimanoj.C

Register Number: 511523205056

Institution: P.T.Lee Chengalvaraya Naicker College Of Engineering and Technology

Department: Information Technology

Date of Submission: 2020-04-26

1. Problem Statement

Credit card fraud has become a significant threat in the digital age, with billions lost annually to fraudulent transactions.

This issue not only affects financial institutions but also undermines consumer trust in digital payments. As transactions grow

in volume and complexity, traditional rule-based systems struggle to adapt and identify emerging fraud patterns effectively.

An AI-driven solution is essential to enhance detection, reduce false positives, and prevent financial losses while maintaining

seamless user experiences.

2. Objectives of the Project

- Develop an AI-based system for real-time detection and prevention of credit card fraud.
- Minimize false positives and negatives to enhance user satisfaction.
- Identify and adapt to emerging fraud patterns using machine learning techniques.
- Deliver insights and visualizations to help stakeholders understand fraud trends.

3. Scope of the Project

Features to Analyze:

- Transaction amount and frequency.

- Geographic location of transactions.

- Device and browser information.

- Historical transaction behavior.

Limitations:

- Model deployment restricted to API-based systems.

- Use of publicly available datasets to ensure replicability.

- Focus on supervised machine learning techniques.

4. Data Sources

- Dataset Source: Kaggle and UCI repositories.

- Type: Public datasets containing anonymized credit card transactions with labeled fraudulent cases.

- Nature: Static datasets to ensure consistency during development.

5. High-Level Methodology

Data Collection:

Obtain anonymized transaction datasets from reputable public repositories.

Data Cleaning:

Address missing values, remove duplicates, and standardize data formats for consistency.

Exploratory Data Analysis (EDA):

Use visualization techniques like histograms and heatmaps to understand correlations and identify fraud indicators.

Feature Engineering:

Create derived features such as transaction velocity and clustering by geographic location to improve model inputs.

Model Building:

Experiment with machine learning models like Random Forests, Gradient Boosting Machines (GBMs), and Neural Networks to

optimize fraud detection.

Model Evaluation:

Evaluate performance using precision, recall, F1-score, and ROC-AUC metrics to ensure the model balances detection and

false positive rates.

Visualization & Interpretation:

Use tools like Matplotlib and Seaborn to present fraud patterns and model predictions in a digestible format.

Deployment:

Develop an API for real-time transaction scoring using Flask or FastAPI for easy integration with financial systems.

6. Tools and Technologies

Programming Language:

Python

Notebook/IDE:

Jupyter Notebook or Google Colab

Libraries:

- Data Processing: Pandas, NumPy
- Visualization: Matplotlib, Seaborn
- Modeling: scikit-learn, TensorFlow, XGBoost
- Deployment: Flask, FastAPI

7. Team Members and Roles

- Responsible for data cleaning and EDA:Arulirasan.G
- Leads model building and evaluation:Anandharaman.M
- Handles API development and deployment:Srimanoj.C
- Ensures timelines are met and oversees integration with client systems:Thiruneelakandan.M