AISaksham

edunet foundation

Credit Card Fraud Detection

Team Members:

1. Panchal Darshana Narendrakumar
2. Delvadiya Urvisha Vipulbhai
3. Tokare Sumeet Magan

Guide: Jay Rathod

edunet foundation

OUTLINE

- Abstract
- Problem Statement
- Aims, Objective & Proposed System/Solution
- System Design/Architecture
- System Development Approach (Technology Used)
- Algorithm & Deployment
- Conclusion
- Future Scope
- References
- Video of the Project

Abstract

- With the rapid increase in digital transactions, credit card fraud has emerged as a critical issue, causing substantial financial losses and compromising consumer trust. Traditional detection methods often fail to keep up with the evolving tactics of fraudsters. This project aims to address this challenge by employing advanced machine learning algorithms to detect fraudulent credit card transactions. By analyzing transaction data for patterns and anomalies, the model developed in this project provides a robust solution for identifying and mitigating credit card fraud in real-time, ensuring enhanced security and trust in digital payment systems.

edunet foundation

Problem Statement

- Credit card fraud leads to substantial financial losses for individuals and institutions. Traditional fraud detection methods often fail to keep pace with evolving fraudulent techniques. This project aims to develop a machine learning model to identify and prevent fraudulent transactions in real-time. By leveraging the capabilities of Logistic Regression, the model will enhance accuracy and scalability. The solution seeks to address the need for a robust and adaptive fraud detection system in the face of increasing digital transactions.

edunet foundation

Aim and Objective

- Develop a machine learning model to accurately detect credit card fraud.
- Enhance the detection accuracy by preprocessing and balancing the dataset.
- Implement a scalable and real-time fraud detection system using Logistic Regression.
- Identify and highlight common patterns in fraudulent transactions.
- Implement robust data handling practices to ensure data integrity and security.

edunet foundation

Proposed Solution

- The proposed solution leverages machine learning to detect credit card fraud. Logistic Regression is used for its efficiency in binary classification. The dataset undergoes preprocessing to handle missing values and balance class distribution, enhancing model performance. The trained model is deployed using Flask, enabling real-time fraud detection through a REST API. Continuous monitoring and updates ensure the model adapts to emerging fraud patterns, providing a robust and scalable solution.

edunet foundation

System Architecture

1. **Data Collection:** Gather transaction data from the Credit Card Fraud Dataset.

2. **Data Preprocessing:** Clean the data, handle missing values, and balance the classes to prepare for training.

3. **Model Training:** Use Logistic Regression for binary classification of transactions as legitimate or fraudulent.

4. **Model Evaluation:** Assess the model's performance using accuracy, precision, recall, and other relevant metrics.

5. **Model Deployment:** Implement the model as a Flask REST API for real-time fraud detection.

6. **Continuous Monitoring:** Regularly update the model with new data to maintain accuracy and adapt to new fraud patterns.

System Deployment Approach

Technology Used:

Python: Primary programming language for data analysis and model building.
Pandas: Data manipulation and preprocessing.
Scikit-Learn: Model training and evaluation.
Flask: Deployment of the model as a REST API for real-time fraud detection.

Dataset:

Credit Card Fraud Detection dataset: Used for training and evaluating the model.

Tools:

Jupyter Notebook: For interactive coding and data analysis.
IDE: Integrated Development Environment for coding.
Flask: For creating and deploying the API.

edunet foundation

Algorithm & Deployment

Algorithm: Logistic Regression

1. **Load and preprocess the dataset:** Import the credit card transaction data, handle missing values, and normalize or scale features as needed.
2. **Balance the dataset:** Address class imbalances by techniques such as undersampling the majority class or oversampling the minority class to ensure equal representation of fraudulent and non-fraudulent transactions.
3. **Split the data into training and testing sets:** Divide the data into training and testing sets to build and evaluate the model's performance.
4. **Train the Logistic Regression model:** Fit the Logistic Regression model on the training data to learn the patterns associated with fraudulent transactions.
5. **Evaluate the model's accuracy:** Assess the model’s performance on the test set using accuracy, precision, recall, and F1-score to ensure effective fraud detection.
6. **Deploy the model using Flask to create a REST API:** Create a Flask application to deploy the trained model, enabling real-time predictions of transaction fraud through a RESTful API.

edunet foundation

Conclusion

- The Logistic Regression model effectively identifies fraudulent transactions with a high degree of accuracy. The model can be deployed in real-time systems to flag suspicious transactions and reduce financial losses due to fraud.

edunet foundation

Future Scope

- Improve the model by incorporating more advanced algorithms like Neural Networks or Ensemble methods.
- Continuously update the model with new data to maintain its effectiveness.
- Implement the system in real-time transaction monitoring systems for financial institutions.

Reference

- Dal Pozzolo, Andrea, et al. "Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy." *IEEE Transactions on Neural Networks and Learning Systems*, vol. 29, no. 8, 2018, pp. 3784-3797
- Carcillo, Fabrizio, et al. "Scarff: A scalable framework for streaming credit card fraud detection with spark." *Information Fusion*, vol. 41, 2018, pp. 182-194
- Jurgovsky, Johannes, et al. "Sequence Classification for Credit-Card Fraud Detection." *Expert Systems with Applications*, vol. 100, 2018, pp. 105-117.
- Srivastava, A., et al. "Credit Card Fraud Detection using Hidden Markov Model." *IEEE Transactions on Dependable and Secure Computing*, vol. 5, no. 1, 2008, pp. 37-48.
- Whitrow, C., et al. "Transaction Aggregation as a Strategy for Credit Card Fraud Detection." *Data Mining and Knowledge Discovery*, vol. 18, no. 1, 2009, pp. 30-55.
- Phua, Clifton, et al. "A Comprehensive Survey of Data Mining-based Fraud Detection Research." *arXiv preprint arXiv:1009.6119*, 2010.

Credit Card Fraud Detection

Team Members:

1. Panchal Darshana Narendrakumar
2. Delvadiya Urvisha Vipulbhai
3. Tokare Sumeet Magan

Guide: Jay Rathod

edunet foundation

Thank you!