10 Academy: Artificial Intelligence Mastery

Week 8&9 Challenge Document

Date: 16 July - 29 July 2025

Improved detection of fraud cases for e-commerce and bank transactions

Overview

Business Need

You are a data scientist at **Adey Innovations Inc**., a top company in the financial technology sector. Your company focuses on solutions for e-commerce and banking. Your task is to improve the detection of fraud cases for e-commerce transactions and bank credit transactions.

This two-week period is designed to be flexible. For many, this will be an opportunity to take a well-deserved break or catch up on previous challenges. For those who wish to engage with new material, this challenge offers a focused, streamlined project.

This project aims to create accurate and strong fraud detection models that handle the unique challenges of both types of transaction data. It also includes using geolocation analysis and transaction pattern recognition to improve detection. Good fraud detection greatly improves transaction security. By using advanced machine learning models and detailed data analysis, Adey Innovations Inc. can spot fraudulent activities more accurately. This helps prevent financial losses and builds trust with customers and financial institutions.

A key challenge in fraud detection is managing the trade-off between security and user experience. False positives (incorrectly flagging legitimate transactions) can alienate customers, while false negatives (missing actual fraud) lead to direct financial loss. Your models should therefore be evaluated not just on overall accuracy, but on their ability to balance these competing costs. A well-designed fraud detection system also makes real-time monitoring and reporting more efficient, allowing businesses to act quickly and reduce risks**.**

This project will involve:

- Analyzing and preprocessing transaction data.
- Creating and engineering features that help identify fraud patterns.
- Building and training machine learning models to detect fraud.
- Evaluating model performance and making a justified selection..
- Interpreting your model's decisions using modern explainability techniques.

Data and Features

You will be using the following datasets:

1. Fraud_Data.csv

   Includes e-commerce transaction data aimed at identifying fraudulent activities.

   - **user_id**: A unique identifier for the user who made the transaction.
   - **signup_time**: The timestamp when the user signed up.
   - **purchase_time**: The timestamp when the purchase was made.
   - **purchase_value**: The value of the purchase in dollars.
   - **device_id**: A unique identifier for the device used to make the transaction.
   - **source**: The source through which the user came to the site (e.g., SEO, Ads).
   - **browser**: The browser used to make the transaction (e.g., Chrome, Safari).
   - **sex:** The gender of the user (M for male, F for female).
   - **age**: The age of the user.
   - **ip_address**: The IP address from which the transaction was made.
   - **class**: The target variable where 1 indicates a fraudulent transaction and 0 indicates a non-fraudulent transaction.
   - **Critical Challenge**: Class Imbalance. This dataset is highly imbalanced, with far fewer fraudulent transactions than legitimate ones. This will significantly influence your choice of evaluation metrics and modeling techniques.

2. IpAddress_to_Country.csv

   Maps IP addresses to countries

   - **lower_bound_ip_address**: The lower bound of the IP address range.
   - **upper_bound_ip_address**: The upper bound of the IP address range.
   - **country**: The country corresponding to the IP address range.

3. creditcard.csv

   Contains bank transaction data specifically curated for fraud detection analysis.

   - **Time**: The number of seconds elapsed between this transaction and the first transaction in the dataset.
   - **V1 to V28**: These are anonymized features resulting from a PCA transformation. Their exact nature is not disclosed for privacy reasons, but they represent the underlying patterns in the data.
   - **Amount**: The transaction amount in dollars.

- **Class**: The target variable, where 1 indicates a fraudulent transaction and 0 indicates a non-fraudulent transaction.
- **Critical Challenge**: Class Imbalance. Like the e-commerce data, this dataset is extremely imbalanced, which is typical for fraud detection problems.

Learning Outcomes

- Skills:
  - Effectively clean, preprocess, and merge complex datasets.
  - Engineer meaningful features from raw data.
  - Implement techniques to handle highly imbalanced datasets.
  - Train and evaluate models using metrics appropriate for imbalanced classification (e.g., AUC-PR, F1-Score).
  - Articulate and visualize model predictions using explainability tools like SHAP.
- Knowledge:
  - Grasp the business and technical challenges of fraud detection.
  - Understand the importance of model explainability (XAI) for building trust and deriving insights.
  - Justify model selection based on both performance metrics and business context.
- Behaviors:
  - Adopt a business-centric approach to problem-solving.
  - Demonstrate a systematic and organized workflow from data analysis to final interpretation.

Communication:

- Reporting on statistically complex issues

Team

Tutors:

- Mahlet
- Rediet
- Kerod
- Rehmet

Key Dates

- Discussion on the case - 09:30 UTC on Wednesday 16 July 2025. Use #all-week8 to pre-ask questions.
- Interim-1 Submission - 20:00 UTC on Sunday 20 July 2025.
- Interim-2 Submission - 20:00 UTC on Sunday 27 July 2025.
- Final Submission - 20:00 UTC on Tuesday 29 July 2025

Instructions

Task 1 - Data Analysis and Preprocessing

1. Handle Missing Values
    - Impute or drop missing values
2. Data Cleaning
    - Remove duplicates
    - Correct data types
3. Exploratory Data Analysis (EDA)
    - Univariate analysis
    - Bivariate analysis
4. Merge Datasets for Geolocation Analysis
    - Convert IP addresses to integer format
    - Merge Fraud_Data.csv with IpAddress_to_Country.csv
5. Feature Engineering
    - Transaction frequency and velocity for Fraud_Data.csv
    - Time-Based features for Fraud_Data.csv
        i. hour_of _day
        ii. Day_of_week
    - *time_since_signup*: Calculate the duration between *signup_time* and *purchase_time*.
6. Data Transformation:
    - Handle Class Imbalance: Analyze the class distribution. Research and apply appropriate sampling techniques (e.g., SMOTE for oversampling, Random Undersampling) to the training data only. Justify your choice.
    - Normalization and Scaling (e.g., StandardScaler, MinMaxScaler).
    - Encode Categorical Features (e.g., One-Hot Encoding).

Task 2 - Model Building and Training

- Data Preparation:
    - Separate features and target, and perform a train-test split. [‘**Class**’(creditcard), ‘**class**’(Fraud_Data)]
    - Train-Test Split
- Model Selection
    - You are required to build and compare two models:
        - **Logistic Regression**: As a simple, interpretable baseline.

    - **One Powerful Ensemble Model**: Your choice of Random Forest or a Gradient Boosting model (e.g., LightGBM, XGBoost).
- Model Training and Evaluation
    - Train your models on both datasets.
    - Use appropriate metrics for imbalanced data (AUC-PR, F1-Score, Confusion Matrix).
    - Clearly justify which model you consider "best" and why.

Task 3 - Model Explainability

Use SHAP (Shapley Additive exPlanations) to interpret your best-performing model.

- Generate and interpret SHAP plots (e.g., Summary Plot, Force Plot) to understand global and local feature importance.
- In your final report, explain what these plots reveal about the key drivers of fraud in the data.

Tutorials Schedule

Overview

In the following, the colour **purple** indicates morning sessions, and **blue** indicates afternoon sessions.

Wednesday

- Introduction to the challenge (Mahlet)
- Fraud Detection Concepts(Rehmet).

Thursday

- Model Building & Interpretation with SHAP(Rediet)

Friday

- How to communicate insight from data (Kerod)

Monday

- Q&A

Tuesday

- Q&A

Thursday

- Q&A

Monday

- Q&A

Deliverables

Interim - 1 Submission Sunday 20 July, 2025

Focus: The goal is to confirm you have started your analysis and have a basic understanding of the datasets.(Task 1).

- **What to Submit**:
    - **A link to your GitHub repository.**
    - A detailed Report. This report must include::
        - A summary of your data cleaning and preprocessing steps.
        - Key insights and visualizations from your Exploratory Data Analysis (EDA).
        - A clear explanation of your feature engineering choices, especially the time_since_signup and IP address-to-country mapping.
        - Your analysis of the class imbalance problem and your proposed strategy for handling it.

Interim - 2 Submission Sunday 27 July, 2025

- **Focus:** The goal is to confirm you have successfully built and evaluated at least one model. (Tasks 2) .
- **What to Submit**:
    - **A link to your GitHub repository.**
    - Your repo should now reflect the completion of the modeling task in addition to the first interim.

Feedback

You may not receive detailed comments on your interim submission but will receive a grade.

Final Submission Tuesday, 29 July 2025

- Focus: A complete, well-documented, and deployable end-to-end project.
- **What to Submit**:
    - A polished Blog Post (e.g., on Medium) or a formal PDF Report. This document should narrate the entire project story and must include:
        - Your data analysis, feature engineering, and visualizations.

        - A performance comparison of your models with justification for your final choice.
        - Screenshots and your interpretation of the SHAP plots.
    - A link to your final GitHub repository. The repository must be professional and self-contained. It should include:
        - A comprehensive README.md file. This file must contain:
        - A project overview.
        - Instructions on how to set up the environment and run the code.
        - All your code, organized into logical folders.

Feedback

You will receive comments/feedback in addition to a grade.

References

Fraud Detection

1. https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud
2. https://www.kaggle.com/c/ieee-fraud-detection/code
3. https://www.kaggle.com/datasets/vbinh002/fraud-ecommerce/code
4. Fraud Detection
5. https://complyadvantage.com/insights/what-is-fraud-detection/
6. https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-fraud-detection/

Modeling

1. https://www.analyticsvidhya.com/blog/2021/08/conceptual-understanding-of-logistic-regression-for-data-science-beginners/
2. https://www.analyticsvidhya.com/blog/2021/08/decision-tree-algorithm/
3. https://www.analyticsvidhya.com/blog/2021/06/understanding-random-forest/
4. https://www.datacamp.com/tutorial/guide-to-the-gradient-boosting-algorithm
5. https://www.datacamp.com/tutorial/multilayer-perceptrons-in-machine-learning
6. https://www.datacamp.com/tutorial/introduction-to-convolutional-neural-networks-cnns
7. https://towardsdatascience.com/convolutional-neural-networks-explained-9cc5188c4939
8. https://www.ibm.com/topics/recurrent-neural-networks
9. https://www.analyticsvidhya.com/blog/2022/03/a-brief-overview-of-recurrent-neural-networks-rnn/
10. https://www.analyticsvidhya.com/blog/2021/03/introduction-to-long-short-term-memory-lstm/
11. https://machinelearningmastery.com/gentle-introduction-long-short-term-memory-networks-experts/

Model Explainability

1. https://www.larksuite.com/en_us/topics/ai-glossary/model-explainability-in-ai
2. https://www.analyticsvidhya.com/blog/2021/11/model-explainability/
3. https://www.ibm.com/topics/explainable-ai

4. https://www.datacamp.com/tutorial/explainable-ai-understanding-and-trusting-machine-learning-models

Flask and dash

1. https://flask.palletsprojects.com/en/3.0.x/
2. https://www.geeksforgeeks.org/flask-tutorial/
3. https://realpython.com/python-dash/
4. https://dash.plotly.com/layout