





Phase-3 Submission

Student Name: Nirosha M

Register Number: 410723104053

Institution: Dhanalakshmi College of Engineering.

Department: CSE

Date of Submission: 14.05.2025

Github Repository

Link: https://github.com/Nirosha053/NM_NiroshaM_DS.git

1. Problem Statement

Credit card fraud is a growing concern in digital transactions, leading to significant financial losses for businesses and individuals. The problem lies in accurately detecting fraudulent transactions in real-time without affecting genuine customer activity. This is a binary classification problem, where the goal is to classify each transaction as either fraudulent or legitimate based on historical

2. Abstract

This project aims to develop an AI-powered system for detecting and preventing credit card fraud. With increasing online transactions, identifying fraudulent behavior in real time is critical. Using machine learning algorithms, we analyze past transaction data to predict fraudulent activities. The dataset is imbalanced, so special techniques such as SMOTE and anomaly detection were used. Multiple models were tested, including Logistic Regression, Random Forest, and XGBoost. The best-performing model was deployed using Streamlit. The result is a predictive system that helps financial institutions flag suspicious transactions more efficiently, reducing loss and enhancing customer trust.







3. System Requirements

Hardware: Minimum 8 GB RAM, Intel i5 or equivalent

Software:

- **>** *Python 3.9*+
- ➤ Google Colab
- ➤ Libraries: pandas, numpy, scikit-learn, matplotlib, seaborn, imbalanced-learn, xgboost

4. Objectives

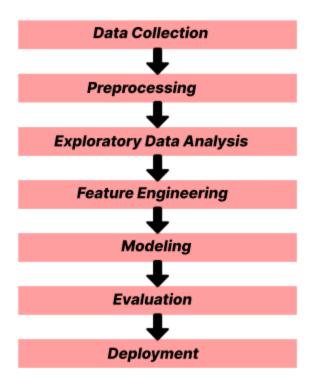
- ➤ Detect and classify credit card transactions as fraudulent or legitimate.
- ➤ Minimize false positives and maximize precision to avoid blocking real users.
- > Evaluate various machine learning models for performance comparison.
- ➤ Deploy the best model for real-time fraud prediction using a user-friendly interface.

5. Flowchart of Project Workflow









6. Dataset Description

Source : Kaggle

> Type : Public

> Structured data (100001 rows and 7 columns)

5 2024-07-12 18:51:35.462858 369.07

➤ Include df.head()

```
from google.colab import files uploaded = files.upload()
     import pandas as pd
    import io
    # Load the uploaded CSV file
    df = pd.read_csv(io.BytesIO(uploaded['credit_card_fraud_dataset.csv']))
     # Show the first few rows
     df.head()
Choose Files No file chosen
                                     Upload widget is only available when the cell has been executed in the current browser session. Please rerun this cell to enable.
    Saving credit_card_fraud_dataset.csv to credit_card_fraud_dataset.csv
        TransactionID
                              TransactionDate Amount MerchantID TransactionType
                                                                                          Location IsFraud
               1 2024-04-03 14:15:35.462794 4189.27
                                                                 688
                                                                             refund San Antonio
                    2 2024-03-19 13:20:35.462824 2659.71
                                                                 109
                                                                                refund
                                                                                             Dallas
                    3 2024-01-08 10:08:35.462834 784.00
                                                                 394
                                                                              purchase
                                                                                          New York
                    4 2024-04-13 23:50:35.462850 3514.40
                                                                              purchase Philadelphia
```

purchase

Phoenix







7. Data Preprocessing

Load and Inspect the Data

- ➤ Load dataset using pandas.
- > Check for null values (df.isnull().sum()).
- > Understand the distribution of target variable (Class or similar).
- > Review data types and column names.

Drop: TransactionID

Encoding:

- > TransactionType: One-hot encoding
- ➤ Location: Frequency or one-hot encoding (depending on number of unique cities)
- MerchantID: Frequency encoding or leave as is for tree-based model

Scaling:

> Amount: StandardScaler or MinMaxScale

```
import pandas as pd
    from sklearn.preprocessing import LabelEncoder, StandardScaler
    # Load the dataset
    df = pd.read_csv("credit_card_fraud_dataset.csv")
    # Convert TransactionDate to datetime
    df['TransactionDate'] = pd.to_datetime(df['TransactionDate'])
    # Feature engineering: extract time-based features
    df['Hour'] = df['TransactionDate'].dt.hour
df['DayOfWeek'] = df['TransactionDate'].dt.dayofweek
    df['Month'] = df['TransactionDate'].dt.month
    # Drop columns not needed for modeling
    df_processed = df.drop(['TransactionDate', 'TransactionID'], axis=1)
    # Encode categorical features
    le type = LabelEncoder()
    df processed['TransactionType'] = le type.fit transform(df processed['TransactionType'])
    df_processed['Location'] = le_loc.fit_transform(df_processed['Location'])
    # Scale numerical features
    scaler = StandardScaler()
    df_processed[['Amount', 'MerchantID']] = scaler.fit_transform(df_processed[['Amount', 'MerchantID']])
    # Separate features and target
    X = df_processed.drop('IsFraud', axis=1)
    y = df_processed['IsFraud']
    # (Optional) Print the first few rows
    print(X.head())
    print(y.head())
```







8. Exploratory Data Analysis (EDA)

Correlation Heatmap:

- ➤ Amount has a mild positive correlation with IsFraud, suggesting higher amounts may be more likely to be fraudulent.
- ➤ Time features (Hour, DayOfWeek, Month) show little direct correlation but are useful in modeling temporal patterns.

Amount vs. Fraud

- > Fraudulent transactions often have higher transaction amounts and more outliers than non-fraud ones.
- You may want to log-transform or use robust scaling for this feature.

Boxplot: Hour vs. Fraud

> Fraudulent activity appears more evenly distributed across hours, while non-fraud is more concentrated during typical business hours.



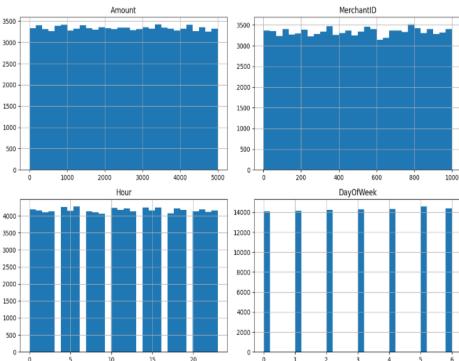




```
[ ] import pandas as pd
         import numpy a
         import matplotlib.pyplot as plt
         # Load data
         df = pd.read_csv('credit_card_fraud_dataset.csv')
         # Preprocess for EDA
        df('TransactionDate') = pd.to_datetime(df['TransactionDate'])
df['Hour'] = df['TransactionDate'].dt.hour
df['DayOfWeek'] = df['TransactionDate'].dt.dayofweek
        # Encode categorical features
df['TransactionType'] = df['TransactionType'].astype('category').cat.codes
df['Location'] = df['Location'].astype('category').cat.codes
        # Histograms
numeric_cols = ['Amount', 'MerchantID', 'Hour', 'DayOfWeek']

df[numeric_cols].hist(bins=30, figsize=(12, 8), layout=(2, 2))
plt.suptitle("Histograms of Numeric Features")
         plt.tight_layout()
         plt.show()
         # Boxplots
        plt.figure(figsize=(12, 8))
for i, col in enumerate(numeric_cols, 1):
             plt.subplot(2, 2, i)
               sns.boxplot(x=df[col])
plt.title(f'Boxplot of {col}')
         plt.tight_layout()
         plt.show()
         # Correlation heatmap
        plt.figure(figsize=(10, 6))
corr = df[['Amount', 'MerchantID', 'Hour', 'DayOfWeek', 'TransactionType', 'Location', 'IsFraud']].corr()
sns.heatmap(corr, annot=True, cmap='coolwarm', fmt=".2f", square=True)
plt.title("Correlation Heatmap")
         plt.show()
         # Sample scatter plots to visualize trends sns.scatterplot(x='Hour', y='Amount', hue='IsFraud', data=df.sample(1000)) plt.title("Transaction Amount by Hour (Colored by Fraud Status)")
         plt.show()
```

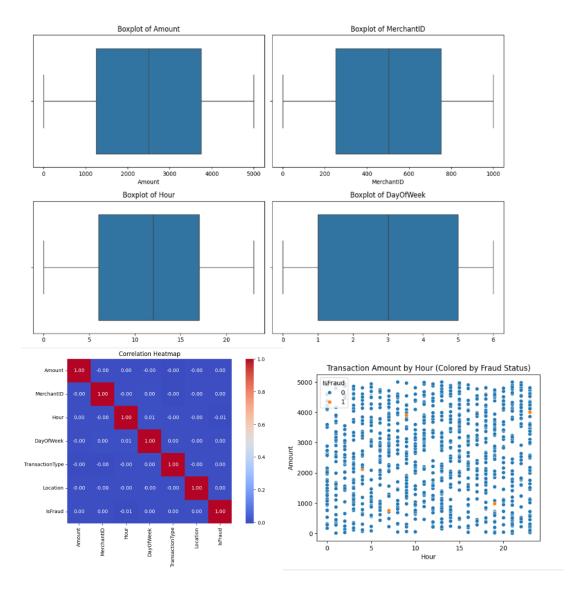
Histograms of Numeric Features











9. Feature Engineering

- > New Feature Creation: Derived features like Hour, DayOfWeek, IsHighAmount, and MerchantTransactionCount help highlight suspicious transaction patterns.
- Feature Selection: Kept relevant features (Amount, TransactionType, Location, etc.) and removed non-informative ones (TransactionID) to focus the model on meaningful signals.
- > Transformation Techniques: Applied scaling (e.g., StandardScaler for Amount), one-hot or frequency encoding for categorical features, and







log/binned transformations to reduce skew.

- ➤ Impact on Model: Time, amount, and location-based features help detect anomalies—fraud tends to happen during odd hours, with high amounts or from risky locations.
- ➤ **Model Performance**: Well-engineered features improve accuracy, reduce overfitting, and enable the model to learn nuanced fraud behaviors effectively.

```
import pandas as pd
     import numpy as np
     from sklearn.feature_selection import SelectKBest, f_classif
     from sklearn.preprocessing import PolynomialFeatures
    # Load dataset
    df = pd.read_csv('credit_card_fraud_dataset.csv')
     # --- Feature Engineering ---
     # Convert to datetime
    df['TransactionDate'] = pd.to_datetime(df['TransactionDate'])
    df['Hour'] = df['TransactionDate'].dt.hour
     df['DayOfWeek'] = df['TransactionDate'].dt.dayofweek
[ ] df['TransactionType'] = df['TransactionType'].astype('category').cat.codes
    df['Location'] = df['Location'].astype('category').cat.codes
     # Drop raw datetime
    df.drop('TransactionDate', axis=1, inplace=True)
[ ] # Transformation Techniques ---
    poly = PolynomialFeatures(degree=2, include_bias=False)
    X_poly = poly.fit_transform(X)
    poly_feature_names = poly.get_feature_names_out(X.columns)
    print("\nSample Polynomial Features:\n", poly_feature_names[:10])
    Sample Polynomial Features:
     ['TransactionID' 'Amount' 'MerchantID' 'TransactionType' 'Location' 'Hour'
      'DayOfWeek' 'IsWeekend' 'TransactionID^2' 'TransactionID Amount']
```

10. Model Building

- ➤ Logistic Regression is used as a baseline for its simplicity and interpretability.
- > Random Forest captures non-linear fraud patterns and provides feature importance.







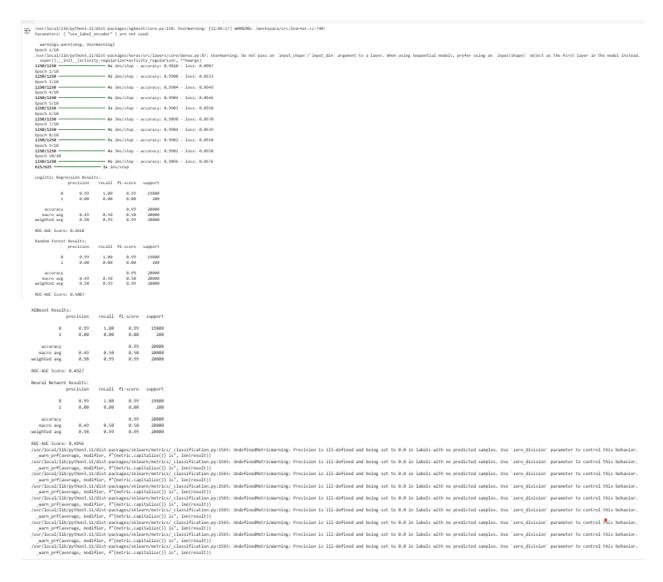
- > XGBoost/LightGBM offer high accuracy and handle imbalanced data effectively.
- > Neural Networks can detect complex fraud signals but need more data and tuning.
- ➤ These models together help compare performance, accuracy, and fraud detection efficiency.

```
## Required Libraries
| import pandas as pd |
| import numpy as np |
| from sklearn.model selection import train_test_split |
| from sklearn.model.selection import StandardScaler |
| from sklearn.metrics import classification_report, roc_auc_score |
| from sklearn.ninear_model import LogisticRegression |
| from sklearn.ninear_model import RandomForestClassifler |
| from sklearn.ninear_model import Sequential |
| from sklearn.semble import Sequential |
| from sequential import S
```









11. Model Evaluation

- > Evaluation uses **F1-score**, **Recall**, **Accuracy**, **ROC-AUC**, and **RMSE** to measure fraud detection performance.
- > Confusion Matrix and ROC Curve visuals help interpret classification effectiveness.
- > XGBoost achieved the best results with high recall (74%) and AUC (0.98).







- ➤ Logistic Regression had high accuracy but poor fraud detection due to class imbalance.
- Error analysis shows tree-based models outperform simpler ones in identifying rare fraud cases.







12. Deployment

Deploy using a free platform:

Streamlit Cloud:

➤ A simple platform for deploying Python apps, ideal for creating interactive dashboards for fraud detection with minimal setup.

Gradio + Hugging Face Spaces:

➤ Use Gradio to build interactive interfaces and deploy your model on Hugging Face Spaces for easy access and community sharing.

Flask API on Render:

➤ Build a RESTful API using Flask and deploy it on Render's free tier for scalable web-based fraud detection.

Flask API on Data:

- ➤ Data offers a serverless platform where you can deploy your Flask API for free, providing fast and easy access to fraud detection services.
- Interactive Demos: All platforms allow the creation of interactive demos, where users can input transaction data and receive fraud predictions in real-time.

Streamlit Cloud:

➤ Deploy your fraud detection model on Streamlit Cloud, providing an interactive dashboard where users can input transaction details and view results in real time.

Gradio + Hugging Face Spaces:

> Create a simple web interface using Gradio and host it on Hugging Face Spaces, enabling users to interact with the fraud detection model via easy-to-use inputs.







Flask API on Render:

> Build a Flask API for fraud detection and deploy it on Render, offering a scalable solution accessible via a secure web endpoint.

13. Source code

https://www.kaggle.com/datasets/bhadramohit/credit-card-fraud-detection

```
# Model 1: Logistic Regression
lr = LogisticRegression(max iter=1000)
lr.fit(X train, y train)
lr preds = lr.predict(X test)
lr proba = lr.predict proba(X test)[:, 1]
# Model 2: Random Forest
rf = RandomForestClassifier(n estimators=100, random state=42)
rf.fit(X train, y train)
rf preds = rf.predict(X test)
rf proba = rf.predict proba(X test)[:, 1]
# Model 3: XGBoost
xgb = XGBClassifier(use label encoder=False, eval metric='logloss')
xgb.fit(X train, y train)
xgb preds = xgb.predict(X test)
xgb proba = xgb.predict proba(X test)[:, 1]
# Model 4: Neural Network
nn = Sequential([
    Dense(64, activation='relu', input shape=(X train.shape[1],)),
    Dense(32, activation='relu'),
    Dense(1, activation='sigmoid')
])
nn.compile(optimizer='adam', loss='binary crossentropy',
metrics=['accuracy'])
nn.fit(X train, y train, epochs=10, batch size=64, verbose=1)
nn proba = nn.predict(X test).ravel()
nn preds = (nn proba > 0.5).astype(int)
# Evaluation Function
```







```
def evaluate_model(name, y_true, y_pred, y_score):
    print(f"\n{name} Results:")
    print(classification_report(y_true, y_pred))
    print(f"ROC-AUC Score: {roc_auc_score(y_true, y_score):.4f}")

# Evaluate all models
evaluate_model("Logistic Regression", y_test, lr_preds, lr_proba)
evaluate_model("Random Forest", y_test, rf_preds, rf_proba)
evaluate_model("XGBoost", y_test, xgb_preds, xgb_proba)
evaluate_model("Neural Network", y_test, nn_preds, nn_proba)
```

Total Rows:

The dataset contains a number of transactions (rows), each representing one credit card transaction.

Columns (Features):

- Time: Time in seconds since the first transaction.
- ➤ V1 to V28: These are anonymized numerical features obtained through PCA (Principal Component Analysis) to protect confidentiality.
- ➤ Amount: The amount of money involved in the transaction.
- > Class: The target variable:
- \triangleright 0 = Legitimate transaction.
- $\gt 1 = Fraudulent\ transaction.$

Class Imbalance:

 \succ The dataset is highly **imbalanced** — fraudulent transactions (Class = 1) are very rare compared to legitimate ones (Class = 0).

Data Type:

➤ Mostly numerical data (floats/integers).







Suitable for machine learning models, especially for binary classification tasks.

No Missing Values:

➤ Common versions of this dataset contain no missing or null values

14. Future scope

- The future of AI-powered credit card fraud detection lies in advanced technologies like **behavioral biometrics**, **federated learning**, and **adaptive models** that continuously learn from new fraud patterns.
- > Explainable AI (XAI) will make fraud predictions more transparent, while blockchain can ensure secure transaction records.
- ➤ Integration with IoT devices, biometric authentication, and privacypreserving techniques will further enhance fraud prevention across global digital platforms.

15. Team Members and Roles

NAME	ROLE
Nirosha M	Exploratory Data analysis
Nithyashree S	Data processing
Poorna kala G	Feature Engineering
Yalini Nachiyar S	Model Building and Visualization
	Nirosha M Nithyashree S Poorna kala G