Fraud Detection in Credit Card Transactions

1. Introduction :-

The widespread use of online transactions and credit cards has led to a significant increase in financial fraud, especially in e-commerce and banking sectors. This project aims to develop a real-time credit card fraud detection system that can help flag suspicious transactions. The system uses machine learning techniques and is accessible via a lightweight web application to ensure easy usability and deployment.

---

2. Abstract: -

This project implements a supervised machine learning model to detect fraudulent credit card transactions based on anonymized transaction data. Leveraging the XGBoost algorithm, the system is trained on highly imbalanced data and evaluated using standard metrics like precision, recall, and ROC AUC. A Flask web application allows users to input transaction features (V1–V28 and Amount) and receive instant fraud detection results. This system offers a scalable and interactive solution for financial fraud prevention.

---

3. Tools Used :-

Programming Language: Python

Libraries/Frameworks:

- **Pandas, NumPy** – For data preprocessing and handling
- **scikit-learn** – For scaling and evaluation
- **XGBoost** – For classification model training
- **Joblib** – For model saving and loading
- **Flask** – For web deployment
- **HTML/Jinja2** – For the user interface

Model: Trained XGBClassifier saved as xgb_model.pkl

---

4. Steps Involved in Building the Project :-

Data Preprocessing:

- Loaded the Kaggle credit card dataset
- Dropped the Time column and scaled the Amount column

- Separated features (V1–V28, Amount) and target (Class)

Anomaly Detection (Optional Step):

- Explored Isolation Forest and Local Outlier Factor for outlier detection
- Gained insights into the behavior of fraudulent transactions

Model Training:

- Used XGBClassifier for its ability to handle class imbalance
- Trained the model using a stratified train-test split
- Achieved strong performance on imbalanced data

Model Evaluation:

- Evaluated using confusion matrix, classification report, and ROC AUC
- Focused on high recall for fraud cases

Model Export:

- Saved trained model using joblib.dump(model, 'xgb_model.pkl')

Web Application:

- Developed a Flask app (app.py)
- HTML form (index.html) captures values for V1–V28 and Amount
- User inputs are processed and predictions displayed in real-time
- UI shows results:
    - Legitimate Transaction
    - Fraudulent Transaction Detected

Deployment:

- App is run using: python app.py
- Interface accessible via browser at: http://127.0.0.1:5000

---

5. Conclusion :-

This project effectively demonstrates the use of machine learning for detecting fraudulent credit card transactions. The integration with Flask enables a simple and functional web interface for real-time prediction. The system can be further enhanced with API integration, transaction logging, or cloud deployment for real-time use in banking systems. It offers a solid foundation for scalable, intelligent fraud detection systems.