Weekly Report – Week 16

Course: Applied Data Science with AI

Semester: BSSE 7th Semester Regular

Week #: 16

Student Name: Amna Tariq

Roll Number: 2225165004

Project Title: 4 → Credit Card Fraud Detection

Report of Credit Card Fraud Detection

1. Introduction and Problem Statement

The rise of **digital banking, online shopping and mobile payments** has revolutionized the way financial transactions are conducted. However, this rapid digitalization has also increased the risk of **credit card fraud**, which poses serious challenges to banks, fintech companies, payment platforms and individual users. Fraudulent transactions can lead to substantial financial losses, damage customer trust and result in reputational harm to financial institutions.

Traditional manual approaches to fraud detection are inefficient due to the **sheer volume of transactions** processed every second and the **rare occurrence of fraud** compared to legitimate transactions. Therefore, **automated fraud detection systems** powered by artificial intelligence (AI) and machine learning (ML) are critical. These systems are capable of analyzing massive datasets, identifying unusual patterns and detecting fraudulent activity in real-time.

Project Aim:

This project focuses on designing and implementing an **end-to-end fraud detection system** using **machine learning, deep learning and unsupervised learning methods**. The system analyzes transaction patterns, predicts fraudulent activities and provides explainable insights for practical applications in the finance sector.

Key Objectives:

1. Preprocess and clean credit card transaction data to ensure reliability.
2. Explore the dataset using visualization and correlation analysis.
3. Identify predictive features most relevant for fraud detection.
4. Build, train and compare **machine learning models** (Logistic Regression, Random Forest).

5. Implement **deep learning models** (ANN, RNN/LSTM) to capture complex patterns.
6. Apply **unsupervised learning** to identify hidden transaction patterns.
7. Deploy the model using **Flask API** for real-time predictions.
8. Integrate **explainability techniques** (SHAP and LIME) for interpretability.
9. Assess the **industry relevance** and ethical considerations of fraud detection systems.

2. Dataset Overview and Preprocessing

Dataset Description:

- The dataset contains **credit card transactions** with **30 columns**, including anonymized features (V1–V28), Amount and Class (target variable).
- Transactions are highly **imbalanced**, with fraudulent transactions making up less than 1% of the data.

Preprocessing Steps:

1. **Data Cleaning:**
    - Removed duplicate and irrelevant rows.
    - Handled missing values by filling or dropping columns where necessary.
    - Treated outliers in the Amount column using the Interquartile Range (IQR) method.
2. **Feature Scaling:**
    - Standardized all numeric features using StandardScaler to ensure uniform scaling.
3. **Exploratory Data Analysis (EDA):**

- Generated visualizations such as histograms, scatter plots, boxplots, bar charts and correlation heatmaps.
- Identified features most correlated with fraud (V12, V14, V17).

4. **Reflection:**
   Preprocessing is a crucial step, as **model performance depends heavily on data quality**. These steps ensured that the dataset was clean, balanced as much as possible and ready for training ML and DL models.

3. Exploratory Data Analysis (EDA)

EDA was performed to better understand the dataset and **identify patterns related to fraudulent transactions**:

- **Fraud vs Non-Fraud Distribution:**
  - Plotted the distribution of the target variable Class to visualize imbalance.
  - Confirmed that fraudulent transactions are extremely rare compared to normal ones.
- **Correlation Analysis:**
  - A correlation heatmap was generated to examine relationships between features and the target variable.
  - Identified top features (V12, V14, V17) that contribute most to fraud prediction.
- **Feature Distributions:**
  - Explored Amount and anonymized features to detect anomalies.
  - Visualizations highlighted patterns in fraudulent behavior that could be used for model training.

Reflection:

EDA helped not only in feature selection but also in understanding the **nature of fraud in financial datasets**, emphasizing the importance of imbalance handling in model design.

4. Machine Learning Models

4.1 Logistic Regression

- Served as a baseline model for classification.
- Simple, interpretable but limited in handling complex feature interactions.

4.2 Random Forest Classifier

- Ensemble of decision trees capable of capturing non-linear patterns.
- Performed better than logistic regression, especially in recall (ability to detect fraud).

Evaluation Metrics:

- Accuracy, Precision, Recall, F1-Score, ROC-AUC.
- Focused on **recall**, as missing fraudulent transactions has a higher cost than false positives.

Reflection:

Machine learning models provided a solid foundation, but deep learning methods were later implemented to capture **deeper, sequential patterns** in transaction data.

5. Deep Learning Models

5.1 Artificial Neural Network (ANN)

- Built using Keras Sequential API with **two hidden layers**.
- Trained on scaled numeric features of transactions.

5.2 Recurrent Neural Network (RNN / LSTM)

- Captured **sequential patterns** in transactions over time.
- Reshaped numeric data into sequences for LSTM layers.

Results:

- ANN improved over Logistic Regression in accuracy and recall.
- RNN provided slightly better recall by learning sequential dependencies, important for time-based fraud detection.

Reflection:
Deep learning models enhanced detection of subtle patterns, demonstrating the **power of neural networks** in financial fraud detection.

6. Unsupervised Learning

Techniques Used:

1. **K-Means Clustering:**
    - Identified hidden clusters in transaction data.
    - One cluster contained a higher proportion of fraudulent transactions.
2. **Principal Component Analysis (PCA):**
    - Reduced dimensionality for visualization in 2D.
    - Enabled visual detection of anomalies and outliers.

Reflection:
Unsupervised learning complemented supervised models, helping **explore hidden structures** and understand fraud patterns not explicitly labeled in the dataset.

7. Model Evaluation

Model	Accuracy	Precision	Recall	F1-Score	ROC-AUC
Logistic Regression	Moderate	Moderate	Low	Moderate	0.81
Random Forest	High	High	High	High	0.93
ANN	High	High	High	High	0.92
RNN/LSTM	High	High	Higher	High	0.94

Insights:

- Recall is prioritized due to the **rare nature of fraud**.
- Random Forest and RNN/LSTM are the **best performing models**.
- Model selection depends on **balance between speed, accuracy and interpretability**.

8. Model Deployment

- Implemented **Flask API** for real-time predictions.
- Endpoint accepts transaction features in JSON format and outputs **fraud probability**.
- Demonstrated live predictions on localhost.

Challenges:

- Large dataset required optimized loading.
- Input shape and JSON format had to match trained model requirements.

Reflection:

Deployment is critical for making AI models **usable in real-world systems**, such as banking apps and fraud monitoring platforms.

9. Explainability and Ethics

Techniques Implemented:

1. **SHAP Values:**
    - Provided global and local explanations for model predictions.
    - Highlighted important features for fraud detection.
2. **LIME:**
    - Explained individual predictions for transactions.

Ethical Considerations:

- Ensured **transparency and fairness**.
- Helped auditors and analysts understand why a transaction was flagged.
- Reduced trust issues with black-box AI models.

Reflection:
Explainability is essential for real-world adoption of AI in finance, ensuring that fraud alerts are **justifiable and actionable**.

10. Industry Relevance

- **Banking:** Real-time transaction monitoring, fraud prevention.
- **Payment Networks:** Visa, Mastercard, PayPal use similar models.
- **E-commerce & Fintech:** Protects online payments, digital wallets (Daraz, Easypaisa, JazzCash).

Benefits:

- Fast detection and fraud prevention.
- Reduces financial losses and chargebacks.
- Builds **customer trust** and strengthens operational efficiency.

- Supports **regulatory compliance** with audit trails and explainable predictions.

Conclusion:

- Developed a comprehensive fraud detection system using **ML, DL and unsupervised learning**.
- Covered **preprocessing, EDA, model building, evaluation, deployment and explainability**.
- Demonstrated industrial relevance and ethical usage in finance.