Payment Fraud Detection Using Machine Learning

A data-driven approach to secure transactions.

Introduction to Payment Fraud

What is Payment Fraud?

- Unauthorized transactions
- Deceptive practices
- Growing concern

Why Machine Learning?

- Detect anomalies
- Real-time analysis
- Reduce financial losses

Dataset Overview

1 Dataset Details

Transaction records with amount, balances, etc.

2 Target Variable

isFraud: 0 (genuine), 1 (fraudulent)

3 Data Mining

Explore transaction features.

Exploratory Data Analysis (EDA)

1

Understand Data

Distribution analysis.

2

Detect Anomalies

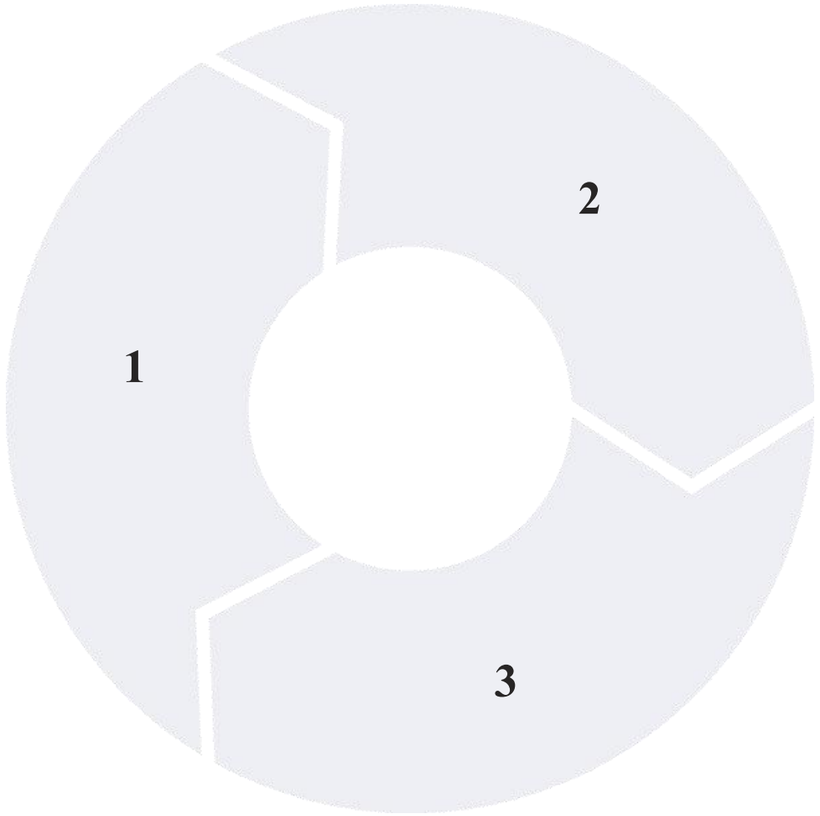
Missing values & outliers.

3

Visualization

Insights from plots.

Feature Engineering



Selection

Choose features.

Transformation

Encode categorical variables.

Data Splitting

70% training, 30% testing.

Machine Learning Models

Logistic Regression

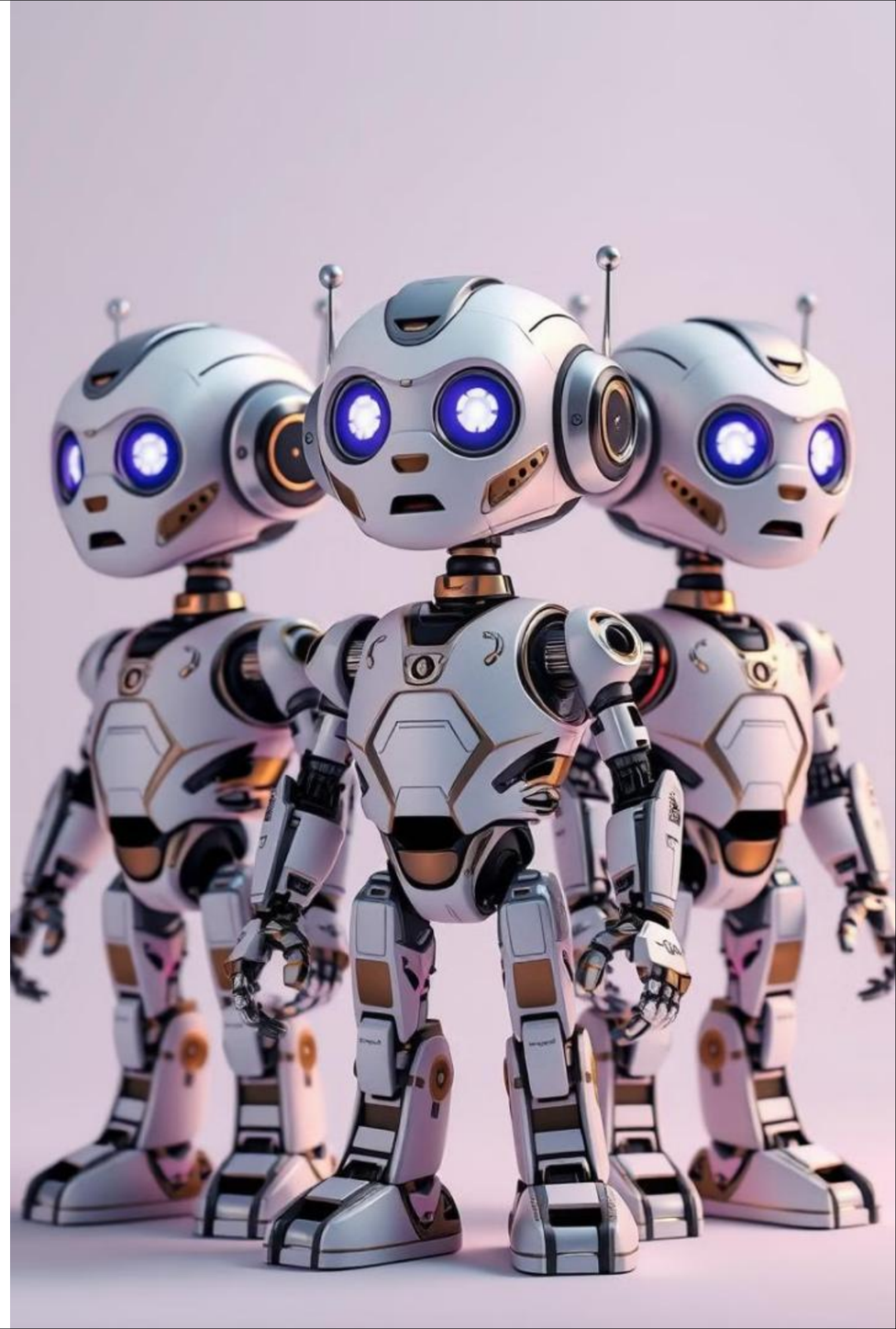
Simple & interpretable.

Random Forest

Ensemble learning.

XGBoost

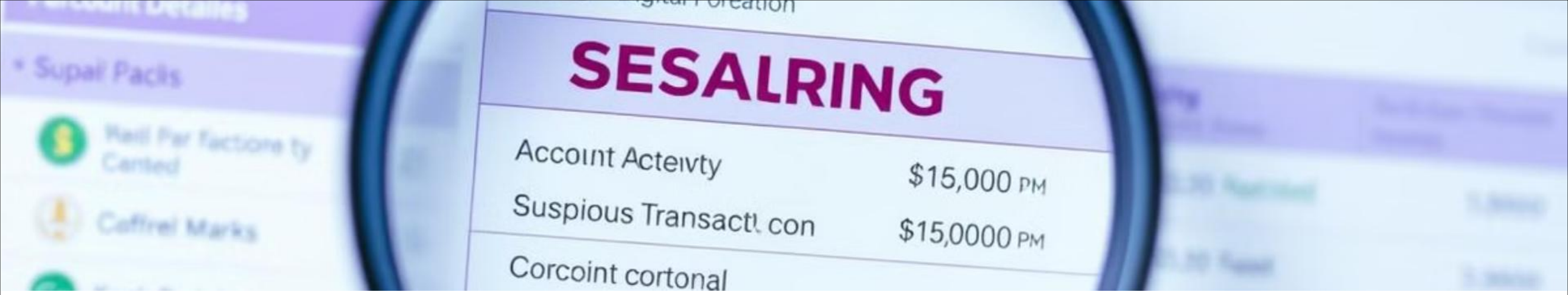
Boosted trees.



Model Evaluation

1. **Accuracy**
2. **Confusion Matrix**
3. **ROC AUC Score**

XGBoost performed best with high fraud detection accuracy.



Key Findings

Unique Patterns

Fraudulent transactions are different.

Crucial Indicators

Account balances are key.

Fraud-Prone Types

Some transactions are riskier.

Future Improvements

1. **SMOTE**

   Balance fraud cases.

2. **Feature Scaling**

   Optimize performance.

3. **Hyperparameter Tuning**

   Improve accuracy.

4. **Ensemble Learning**

   Combine model strengths.

Conclusion & Next Steps

Key Takeaways

- ML can detect fraud
- FE is crucial
- Model optimization matters

Next Steps

- Deploy for real-time detection
- Implement in banking & fintech