

## **Implementation Report**

<b>Date</b>	19 February 2026
<b>Team ID</b>	LTVIP2026TMIDS54062
<b>Project Name</b>	Online Payments Fraud Detection using Machine Learning

### ***Project Title:***

### ***Online Payments Fraud Detection Using Machine Learning***

#### **1. Objective**

The goal of this project is to develop a Machine Learning–based fraud detection system that monitors online payment transactions in real time, identifies suspicious patterns, assigns risk scores, and prevents fraudulent activities before financial loss occurs.

The system is designed to support payment gateways, banks, UPI platforms, and digital wallet providers by providing:

2. Real-time fraud detection
3. Risk-based transaction approval
4. Reduced false positives
5. Regulatory-compliant monitoring

#### **Implementation Phases**

##### **Phase 1: Data Acquisition and Preparation**

###### **Data Sources:**

- Historical transaction records
- Payment gateway logs
- Customer profile data
- Device fingerprint data
- IP & Geo-location data
- Blacklist databases

###### **Data Preprocessing:**

- Removed missing and duplicate transactions
- Handled imbalanced dataset (Fraud vs Non-Fraud)
- Standardized categorical variables
- Encoded features (One-hot / Label encoding)
- Created derived features such as:
  - Transaction Velocity
  - Average Spending Pattern
  - Location Deviation Score
  - Device Risk Index
  - Behavioral Risk Score

## **Phase 2: Feature Engineering**

Extracted meaningful fraud indicators:

### **Transaction Features:**

- Transaction amount
- Merchant category
- Time of transaction
- Payment method

### **Behavioral Features:**

- Frequency of transactions
- Sudden change in spending
- Multiple transactions in short time

### **Device & Network Features:**

- IP mismatch
- New device detection
- Geo-location anomaly
- VPN / Proxy detection

These features were stored in a **Feature Store** for consistent model training and scoring.

## **Phase 3: Model Development**

### **Machine Learning Models Used:**

#### **Supervised Learning Models:**

- Logistic Regression
- Random Forest
- XGBoost

#### **Anomaly Detection Models:**

- Isolation Forest
- Autoencoders

#### **Model Evaluation Metrics:**

- Accuracy
- Precision
- Recall
- F1-Score
- ROC-AUC Curve

Special focus was given to:




- Maximizing Recall (to detect fraud cases)
- Minimizing False Positives (to avoid blocking genuine users)

## **Phase 4: Real-Time Fraud Detection Engine**

Implemented:

- Real-time API-based transaction scoring
- Risk score calculation (0–100 scale)
- Hybrid scoring approach:
  - ML model probability
  - Rule-based engine score

### **Risk Categorization:**

-  High Risk → Block Transaction
-  Medium Risk → Step-up Authentication (OTP / 3D Secure)
-  Low Risk → Approve Transaction

## **Phase 5: Dashboard & Monitoring**

Developed monitoring dashboards for:

- Fraud Rate (%)
- Daily Suspicious Transactions
- Risk Distribution
- Model Performance Metrics
- Alert System for High-Risk Transactions
- Model Drift Detection

Stakeholders involved:

- Fraud Analysts
- Risk Management Team
- Compliance Officers
- Payment Operations Team

## **Key Insights Delivered**

- Fraud transactions often occur in rapid bursts (velocity-based detection is critical).
- New device + high transaction amount significantly increases fraud probability.
- Night-time cross-border transactions show higher fraud risk.
- Combining ML models with business rules improves detection accuracy.

## **Tools and Technologies Used**

### **Programming:**

Python

### **Libraries:**

Pandas, NumPy, Scikit-learn, XGBoost, TensorFlow

### **Streaming & Processing:**

Kafka / Spark Streaming

### **Database:**

MySQL / PostgreSQL

### **Model Deployment:**

Flask / FastAPI

### **Visualization & Monitoring:**

Power BI / Tableau / Custom Dashboard

### **Cloud (Optional):**

AWS / Azure / GCP

## **Outcomes**

- Built scalable real-time fraud detection system
- Reduced fraud losses
- Improved transaction approval speed
- Achieved balanced Precision & Recall
- Enabled automated risk-based decision-making
- Enhanced customer trust in digital payments

## **Next Steps**

- Implement Graph-based fraud detection (network fraud rings)
- Add behavioral biometrics (keystroke, touch pattern analysis)
- Deploy adaptive models with online learning
- Integrate explainable AI (SHAP) for regulatory transparency
- Implement federated learning for cross-bank fraud intelligence

## **Conclusion**

The project successfully demonstrates how Machine Learning can transform traditional rule-based fraud systems into intelligent, adaptive, and real-time fraud prevention platforms.

By combining predictive modeling, behavioral analytics, and automated risk scoring, the system ensures secure, scalable, and efficient online payment processing.