Report: Super OTP Eligibility Predictor

Introduction

In the evolving world of digital payments and app-based transactions, authentication plays a critical role in ensuring both security and user experience. Traditionally, users receive a One-Time Password (OTP) via SMS or email to complete a transaction. While this method is reliable, it introduces delays, dependency on external networks, and is vulnerable to SIM swap or interception attacks.

To address these concerns, the concept of Super OTP has emerged. Unlike traditional OTPs, Super OTPs are instantly generated within the app using contextual and behavioral signals such as device trust, location match, login patterns, and transaction context. This approach enhances speed, security, and convenience, especially for low-risk users.

The objective of this project is to simulate and build a machine learning-based decision system that predicts whether a user is eligible for Super OTP (1) or should default to the traditional Standard OTP (0). Since no public dataset exists for this problem, we simulate realistic transaction data and train a binary classification model that acts as a lightweight fraud-risk engine. The system considers behavioral factors and financial thresholds (e.g., payment cap of ₹5000) to make fast, safe, and smart OTP decisions.

Dataset Simulation Logic

Since no public dataset exists for Super OTP scenarios, I generated 10,000 transactions with realistic user behavior using Python (faker, random, numpy).

Features:

Column	Type	Description
device_type	Categorical	"Mobile", "Desktop"
location_match	Binary	1 if GPS matches billing address
app_login_duration	Numeric	Minutes since login
app_usage_today	Numeric	Minutes of app usage
payment_amount	Numeric	₹50–₹25,000

transaction_hour	Numeric	0–23
past_fraud_flag	Binary	1 if user had past fraud
network_type	Categorical	"WiFi", "4G", "None"
os_version	Categorical	"Android 12", "iOS 15", etc.
battery_level	Numeric	0–100
eligible_for_super_otp	Binary	Target variable

Super OTP Eligibility Rules

A transaction is eligible for Super OTP (1) if:

- Device is Mobile
- GPS matches billing address
- Logged in ≥ 5 minutes ago
- App used ≥ 20 minutes today
- Battery ≥ 20%
- No past fraud history
- Network is WiFi or 4G
- Payment amount ≤ ₹5000

Model Training & Evaluation

I used scikit-learn's Random Forest Classifier due to its interpretability and robustness for tabular data.

Preprocessing:

- Label encoding of categorical features
- Train-test split: 80/20
- Model: RandomForestClassifier(n_estimators=100, random_state=42)

Evaluation Metrics:

Metric	Score
Accuracy	100%
F1 Score	1.0
Precision	1.0
Recall	1.0

The model achieved perfect scores because the data generation followed consistent logic with no label noise. This result is expected for simulated, rule-driven datasets.

Feature Insights

payment_amount, device_type, battery_level, app_usage_today,and payment_amount were among the most critical predictors.

A bar chart was used to visualize feature importance in the training notebook.

Streamlit Interface (UI)

We built a simple Streamlit app to test eligibility in real-time:

- Clean, double-column UI
- Real-time sliders
- Instant prediction and decision message

This app allows businesses or testers to simulate new transactions and see Super OTP decisions without code.

Conclusion

The Super OTP Eligibility Predictor successfully demonstrates how contextual and behavioral signals can be combined with machine learning to make smart, secure authentication decisions during digital transactions. By simulating realistic user activity and applying logical eligibility rules, we trained a highly accurate binary classification model capable of predicting whether a user should receive a Super OTP or a traditional Standard OTP. The system incorporates an additional financial safeguard by allowing Super OTPs only for transactions below ₹5000, ensuring minimal risk even in edge cases. The user interface built with Streamlit enables real-time, intuitive testing of various transaction scenarios. Overall, this project offers a scalable and efficient approach for enhancing authentication mechanisms while maintaining both security and user convenience.