SCTR’S PUNE INSTITUTE OF COMPUTER TECHNOLOGY

TECHFIESTA’26

INTERNATIONAL HACKATHON

CODE. CREATE. CONQUER

Problem Statement ID	**:**	**FD003**
Problem Statement Title	**:**	**Fake Transaction Detector - Spot the Anomaly!**
PS Domain	**:**	**Fintech**
Team ID	**:**	**207**
Team Name	**:**	**Root_Access**

CERBERUS

The Tri-Shield Fraud Defense

Concept: Hybrid "Glassbox" Detection

- **Cerberus Architecture:** A unique **3-layer defense system** that combines deterministic rules with probabilistic AI.

- **Tri-Shield Core:**
    1. **Rule Engine:** Catches known/fixed patterns (e.g., limit breaches).
    2. **Supervised AI (LightGBM):** Learns complex, non-linear fraud history.
    3. **Unsupervised AI (Isolation Forest):** "Zero-Day" anomalies never seen before.

Key Innovations (USP):

- **"Glassbox" Explainability:** Unlike standard "Blackbox" AI, Cerberus tells you *why* a transaction is flagged (e.g., *"Reason: Impossible Travel Speed > 800km/h"*).

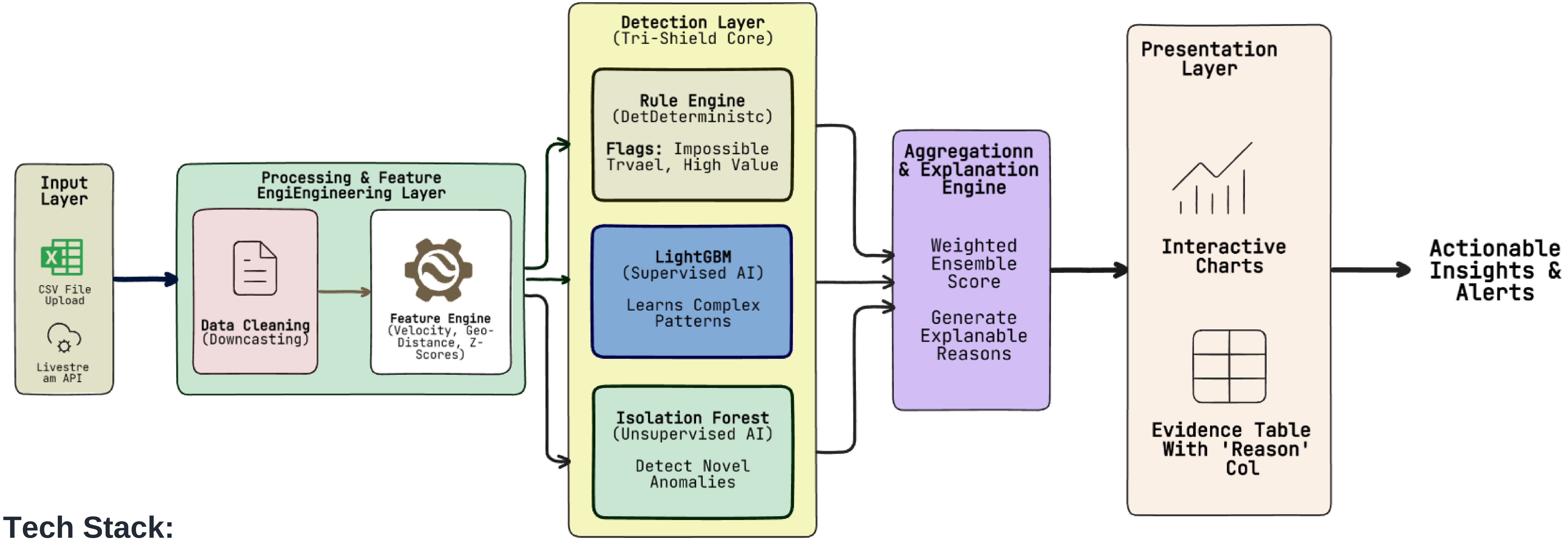
- **Impossible Travel Detection:** Real-time geospatial velocity checks to stop teleportation attacks (Mumbai to London in 10 mins).

- **Velocity & Device Profiling:** Tracks rapid bursts and shared device attacks (botnets).

Objective:

To develop a **real-time, 'Glassbox' fraud detection system** that eliminates AI ambiguity by combining deterministic rules with hybrid machine learning. Our goal is to proactively detect sophisticated financial attacks while providing **transparent, human-readable explanations** for every flagged transaction

TECHNICAL APPROACH



Input Layer

CSV File Upload

Livestre am API

Processing & Feature EngiEngineering Layer

Data Cleaning (Downcasting)

Feature Engine (Velocity, Geo-Distance, Z-Scores)

Detection Layer (Tri-Shield Core)

Rule Engine (DetDeterministc)

Flags: Impossible Trvael, High Value

LightGBM (Supervised AI)

Learns Complex Patterns

Isolation Forest (Unsupervised AI)

Detect Novel Anomalies

Aggregationn & Explanation Engine

Weighted Ensemble Score

Generate Explanable Reasons

Presentation Layer

Interactive Charts

Evidence Table With 'Reason' Col

Actionable Insights & Alerts

Tech Stack:

- **ML(Machine Learning):** Python, Pandas, LightGBM, Isolation Forest, Matplotlib, numpy.
- **Backend:** JAVA, SpringBoot, RestApi, FastApi, Phi3(SLM), axios.
- **Frontend:** HTML, CSS, Javascript.

FEASIBILITY AND VIABILITY

Scalability & Performance:

- Lightweight Compute: LightGBM is highly optimized for CPU. No expensive GPUs required for inference.
- Memory Efficient: Data types downcasted (INT 64 -> UINT 16)to reduce RAM usage by 40%.
- Real-time Ready: Feature engine designed for millisecond latency**.**

Challenges & Mitigation Strategies:

- **Challenge**: "Cold Start" (New users with no history).
  - **Solution**: The Rule Engine acts as the primary defense until history is built.
- **Challenge**: Concept Drift (Fraud patterns changing).
  - **Solution**: The Isolation Forest (Unsupervised) flags novel anomalies automatically, triggering retraining.
- **Challenge**: False Positives annoying customers Solution.
  - **Solution**: Glassbox Explainability + Ensemble Scoring reduces unnecessary blocks by requiring consensus across rules and AI before flagging.

IMPACT AND BENEFITS

Target Audience:

- Small businesses & startups handling online payments
- Fintech learners & student developers
- Small financial platforms without advanced fraud systems
- Operations & audit teams monitoring transaction logs

Impact on Targeted Audience:

- Enables small businesses to detect fraud without enterprise tools
- Helps startups protect users and build early trust
- Empowers operations teams with faster fraud investigation
- Reduces workload for audit and compliance teams
- Gives students real-world exposure to production-grade fraud systems
- Improves decision-making with clear, explainable insights

Key Benefits :

- Detects both known fraud and zero-day anomalies
- Combines rules + AI for higher accuracy
- Provides clear reasons for every flagged transaction
- Reduces false positives compared to rule-only systems
- Works in real-time or batch mode
- Lightweight and deployable on low-cost infrastructure
- Improves audit efficiency with evidence-backed decisions
- Easily customizable rules for different business needs
- Scales from student projects to production pilots

RESEARCH AND REFERENCES

Academic Research Papers:

1. **Anomaly Detection Comparison (2024):**
    1. Thimonier, H., et al. *"Comparative evaluation of anomaly detection methods for fraud detection in online credit card payments."* International Congress on Information and Communication Technology.
    2. **Link:** library.oapen.org/handle/20.500.12657/87000
2. **LightGBM (The Core Model):**
    1. Ke, G., et al. *"LightGBM: A Highly Efficient Gradient Boosting Decision Tree."* (NIPS 2017).
    2. **Link:** papers.nips.cc/paper/6907-lightgbm
3. **Isolation Forest (Unsupervised Layer):**
    1. Liu, F. T., et al. *"Isolation Forest."* (IEEE ICDM 2008).
    2. **Link:** ieeexplore.ieee.org/document/4781136

Our Prototype Link

Project Detail Documentation Link:

- https://heliotrope-deposit-b52.notion.site/28246bcc997380ff95ddee06ce469d8e?v=2cf46bcc997380cfbba3000c793f4dc4&source=copy_link

Prototype Code Link:

https://github.com/Abhinay2007/PICT_Hackthon_Fraud_Detection.git