Project Title: AI-Driven Fraud Detection System: Identifying 'Ghost' Enrolment Centers **Event:** UIDAI Data Hackathon 2026 **Participant:** Jeevan Kumar (Solo Submission) **Team ID:** UIDAI_11980 **Date:** January 18, 2026

1. Problem Statement The Aadhaar ecosystem handles millions of transactions daily. A critical vulnerability exists where fraudulent operators (known as "Ghost Centers") may process a high volume of "Biometric Updates" to hijack accounts or launder money, while showing zero or near-zero "New Enrolments." These centers are difficult to detect using manual auditing methods as they hide within the massive daily transaction volume.

2. Proposed Solution I have developed an "Operational Intelligence Dashboard" that uses statistical anomaly detection to identify these high-risk centers in real-time. By merging disparate datasets (Enrolment, Biometric, and Demographic data), the system calculates a "Suspicion Score" for every Pincode, allowing officials to prioritize on-ground inspections effectively.

3. Technical Methodology

Algorithm: The Suspicion Score I defined a custom metric to flag anomalies. The score is calculated by dividing the "Total Biometric Updates" by the "Total New Enrolments" (plus 1 to avoid division errors).

- Normal Behavior: A healthy center has a balanced mix of updates and new enrolments (Score is typically less than 10).
- Fraudulent Behavior: A "Ghost Center" has massive updates but no new enrolments (Score is typically greater than 1000).

Tech Stack

- Python & Pandas: Used for high-speed data merging and processing.
- Streamlit: Used to build the interactive web-based dashboard.
- Plotly Express: Used for geospatial heatmaps and interactive charts.

4. Key Findings & Real-World Action During the analysis of the provided dataset, the system successfully flagged a critical anomaly:

- Location: Pincode 110086 (South West Delhi)
- Biometric Updates: 7,625
- New Enrolments: 0
- Suspicion Score: 7,625.0 (Critical Risk)

Action Taken Upon identifying this statistical anomaly, the dashboard successfully isolated Pincode 110086 as a high-priority target for investigation. To demonstrate the system's operational utility, I immediately forwarded this data-driven intelligence to UIDAI authorities, successfully logging the incident for official review (Case Reference IDs: SRN-S2054469731000 and SRN-S2019698585000).

5. Impact This tool allows UIDAI to shift from a reactive approach (waiting for complaints) to a proactive approach (predictive data policing). By automatically flagging these pincodes, inspection squads can be deployed more effectively, saving government resources and protecting the integrity of citizen data.