Overview

The Voice Security Dashboard is an interactive web app built to visualize fraudulent and suspicious call activity across telecom networks. It helps users spot trends, identify high-risk patterns, and understand how calls are being handled in real time.

I designed this dashboard as the visual analytics layer of a larger Enterprise Inbound Call Filtering System. While the backend focuses on detecting and classifying threats, the dashboard translates that data into clear, meaningful visuals that make it easier for analysts to act quickly.

Key Features

- **Fraud Type Breakdown:** Pie chart showing spoofed calls, robocalls, IRSF, and Wangiri attempts.
- **Severity Overview:** Visualizes incidents labeled as suspicious, significant, or critical.
- **Call Treatment Analysis:** Compares allowed, flagged, and blocked calls over time.
- **Global Threat Map:** Interactive Leaflet map highlighting the origin of fraudulent calls.
- **Carrier & Time Trends:** Tracks which carriers or time periods experience unusual activity.

How It Fits into the Bigger System

The dashboard connects to data generated by the Enterprise Inbound Call Filtering Platform, which includes several backend components working together to detect and prevent fraud:

Component	Purpose
E-SBC (Session Border Controller)	Manages inbound SIP traffic and applies trust-level policies.
TQ_Trust Server	Executes filtering logic and sends data to the dashboard through REST APIs.
Forensics Server	Logs call metadata and exposes endpoints for analytics.

Fraud Detection Engine	Identifies IRSF and Wangiri call patterns.
Deep-Fake Detection Module	Flags calls with synthetic or spoofed voice signatures.
Reputation Management System	Tracks caller reputation and prevents mislabeling.

Example Use Case

When an inbound call comes through the E-SBC, the TQ_Trust Server decides whether to allow, block, or flag it. The Forensics Server records call metadata such as source country, carrier, and timestamp. That data is then picked up by the Fraud Detection Engine, categorized by type and severity, and displayed in the dashboard—instantly updating charts and maps for the user.

Technology Stack

Layer	Tools
Frontend	React + TypeScript (Vite)
Charts	Recharts
Maps	Leaflet + React-Leaflet
Styling	CSS Grid + Flexbox
Data Source	Local CSV mock data (structured for API integration later)

Integration with Enterprise Call Filtering

The dashboard is meant to complement a larger system for voice-fraud prevention. That system handles the heavy lifting—things like call reputation scoring, deep-fake voice detection, and inbound call trust evaluation—while the dashboard provides an intuitive front-end interface for visualizing it all.

By connecting backend intelligence with a clean, responsive UI, the platform gives analysts a complete view of call security, from real-time alerts to historical analysis.

What the Project Achieves

- Turns complex telecom threat data into easy-to-read visuals.
- Helps identify fraud patterns before they escalate.
- Scales easily to integrate with APIs and databases.
- Provides a professional, production-ready dashboard layout for enterprise use.