HACK4DELHI

Pitch Directly to the Government. Build for the Nation.

Team Name :

The Shadow Brokers

Members name and Affiliation:

Aashi Gupta
Suraj Arya
Mritunjay Kumar
Tanishk Tiwari

Cluster Innovation Centre
University of Delhi

PROBLEM STATEMENT

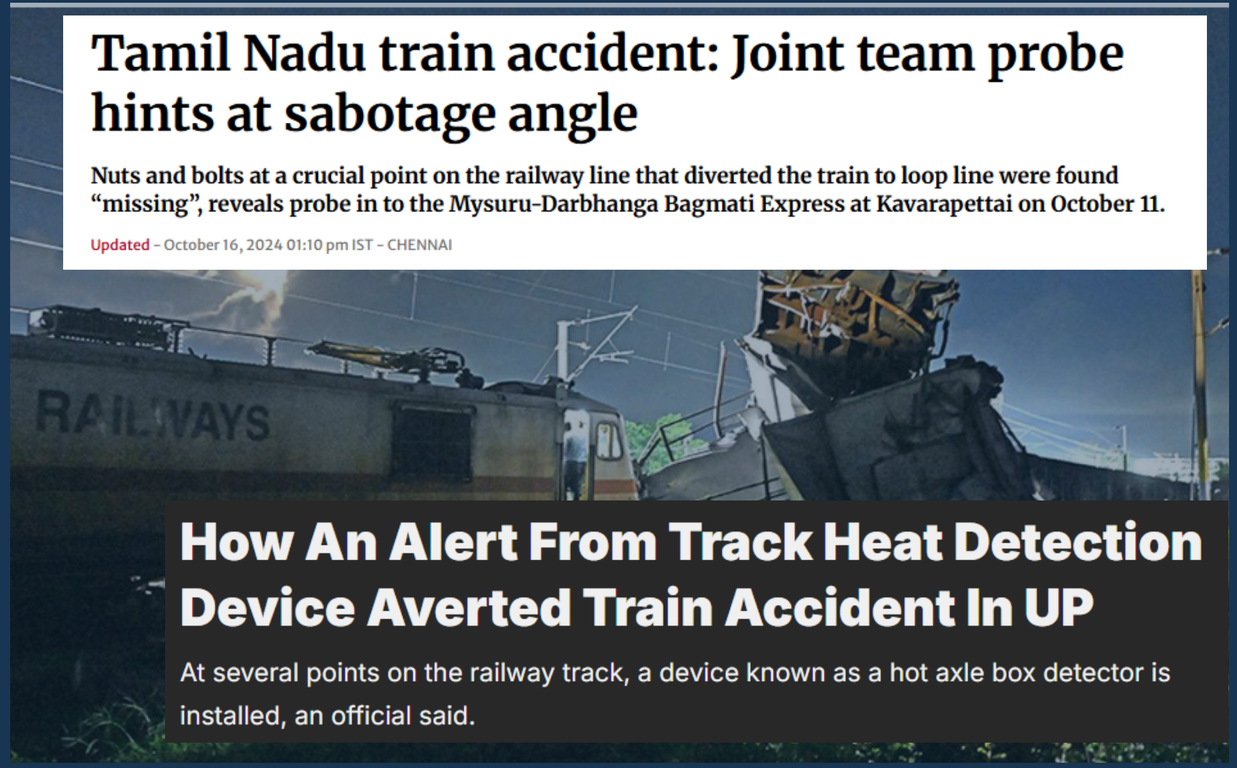
IEEE NSUT

Railway tracks are critical national infrastructure, yet remain physically exposed to intentional tampering such as rail cutting, bolt/fishplate removal, and track obstruction. These incidents usually occur in remote or unmanned sections, at **night or low-visibility between manual patrol intervals**.

Why current systems fail:

- Manual patrols are infrequent and human-dependent
- CCTV systems are high-power, bandwidth-heavy, and weak at night
- Drones provide periodic, weather-dependent monitoring
- Track circuits detect faults, not tampering intent
- Single-sensor setups cause false alarms from rain, animals, or trains

As a result, tampering is often detected only after a derailment or near-miss, making today's response reactive instead of preventive.



This Problem Must Be Solved

- **Safety:** Prevent derailments and loss of life
- **Security:** Railway tracks are soft targets for sabotage
- **Economic Impact:** Avoid massive service disruption & repair costs
- **Scalability:** Thousands of kilometers cannot be manually monitored

IEEE NSUT

SOLUTION

- Decentralized, AI-powered IoT system for real-time detection of intentional track tampering
- Detects the act of tampering, not post-damage failure
- Designed for remote, low-power, large-scale railway deployment

Track Sensors
(Vibration + Audio + Magnetic + Tilt)
↓
Edge AI (TinyML on ESP32)
• Filters trains/weather
• Detects tool signatures
↓
3-Stage Lock Verification
(Vibration + Audio + Magnetic)
↓
Secure Transmission (MQTT over LoRa / LTE)
↓
Central AI Validation (FastAPI)
↓
Real-Time Alert + Evidence Dashboard

Problem	Our Solution
False alarms from rain/animals	Multi-sensor “3-Stage Lock”
Late detection (after derailment)	Detects sawing/hammering in real time
No visibility for officials	Evidence-backed alerts
Remote areas lack connectivity	LoRa + buffering + burst upload
High power CCTV systems	Wake-on-threat, 90% power saving
Drones provide only periodic & weather-dependent surveillance	Ground-mounted, weather-independent sensors
Manual patrols are infrequent & human-dependent	Continuous automated monitoring (24×7)
Track circuits detect faults, not intent of tampering	Intent-aware sensing using vibration + acoustic patterns

Layer	Innovation
Edge	TinyML + FFT on ESP32 (no raw streaming)
Logic	Multi-modal intent detection
Power	Sleep 99%, wake only on threat
Cost	~₹5,200 per node (scalable nationwide)

A practical, low-cost AI system that prevents railway sabotage instead of investigating accidents.

IEEE NSUT

ARCHITECTURE

1. Edge Layer (On-Track Node)
(ESP32 + Sensors)
Sensors collect:
• Vibration + Audio + Magnetic + Track Tilt

FFT + TinyML classify:
- Normal activity (train, weather)
- Abnormal activity (tampering)

Only suspicious events move forward

↓

2. Messaging & Communication Layer
MQTT Publish (QoS-1)
Topic: railway/track_id/data

Reliable delivery using:
- QoS Level 1
- Local FIFO buffering
- Burst transmission after reconnection

↓

Publish–Subscribe Model (MQTT)
- Sensor nodes publish data to topics
- Backend subscribes to all track events
- Decoupled, scalable, fault-tolerant

Time Accuracy
- NTP synchronization on ESP32
- Timestamps generated at event time, not upload time

Data Integrity
- FIFO buffering during network loss
- Burst transmission after reconnection
- QoS Level 1 ensures alert delivery
- Unique message IDs prevent duplicate alerts

- **Edge-first AI** → low latency, low bandwidth
- **MQTT + buffering** → works in remote rail sections
- **Time-series DB** → accurate forensic analysis
- **WebSocket alerts** → instant operational response

3. Cloud & Processing Layer
MQTT Broker receives events
(Mosquitto / HiveMQ)
↓
Backend API
(Python FastAPI)
- Performs multi-sensor AI fusion
- Validates tampering confidence
- Generates structured alerts

↓

Data storage:
• InfluxDB (sensor data)
• PostgreSQL (alerts)

↓

4. Control Room Layer
React.js dashboard
WebSocket-based live alerts
(React.js + WebSockets)
Displays:
- Alert location
- Severity
- Sensor evidence
- Timeline of events

IEEE NSUT

TECHNOLOGY USED

Edge & Sensing Technologies

Component	Technology	Contribution
Edge Controller	ESP32 / STM32	Low-power edge processing, deep sleep, supports on-device AI
Vibration Sensor	ADXL345	Detects cutting, hammering, abnormal rail vibrations
Audio Sensor	INMP441	Identifies grinder / hacksaw acoustic signatures
Magnetic Sensor	HMC5883L	Detects bolt or metal removal (silent tampering)
Edge Intelligence	TinyML + FFT	Local anomaly detection, reduces latency & bandwidth

Visualization & Alerts

Layer	Technology	Contribution
Frontend	React.js + Tailwind CSS	Fast, responsive control-room dashboard
Live Alerts	WebSockets (Socket.io)	Instant alert delivery without page refresh

Communication & Backend Technologies

Layer	Technology	Contribution
Communication	MQTT (LoRaWAN / Wi-Fi / LTE)	Lightweight, scalable, reliable in unstable networks
Message Broker	Mosquitto / HiveMQ	Decouples sensors and backend, supports large-scale deployment
Backend API	Python (FastAPI)	High-performance async processing & AI integration
Real-Time DB	InfluxDB	Efficient storage of high-frequency sensor data
Operational DB	PostgreSQL	Stores alerts, node metadata, system logs

The tech stack is optimized for low power, real-time detection, scalability, and deployment in remote railway environments.

IEEE NSUT

FEATURE/USP

The "False Alarm" Solution

- Doesn’t rely on single sensor
- Alert is generated if all sensors agree

Actionable Intelligence

- Existing dashboards show blinking red dot on map
- Our dashboard delivers proof, not just problems

The "Sleepy Sentinel" Power Architecture

- CCTV requires massive power and expensive cables.
- Our high-power sensors wake up for 10 seconds, when the low-power vibration sensors detect anomaly.

Tamper-Proof" Security

- Criminals cut the wires of security systems.
- Even if the device is destroyed, the circuit sends a final distress signal.
- Magnetic sensor detects if the track components(bolts / fishplates) are removed

Feature	Standard Competitor	Solution
Detection Method	Vibration Only (Single Modality)	**Quad-Fusion (Vibration + Audio + Mag + Vision)**
Verification	None (Guesswork)	**Visual & Audio Proof** included in alert
Power Source	Grid / Heavy Solar	**Micro-Solar / Battery** (Sleep Mode Focus)
Connectivity	High Bandwidth (Fiber/4G)	**Low Bandwidth (LoRa)** + 4G Burst
False Alarms	High (Weather/Animals)	**Near Zero** (Cross-validated)

Cost-to-Coverage Ratio

- Fiber optic sensing (DAS) costs millions per kilometer, while patrolmen are expensive and slow.
- Using mass-produced MEMS sensors, per-node cost of ~₹5,200 ($60) achieved.

IEEE NSUT

REFERENCES/LINKS

- **AI-powered TrackEi™ (L&T Technology Services):** High-speed, AI-enabled rail inspection using cameras and laser profiling for real-time defect detection and maintenance planning.
- **Track Geometry Cars:** Sensor-equipped inspection vehicles widely used for automated track measurement (alignment, twist, gauge) without disrupting operations.
- **Track IQ (Wabtec):** Multi-sensor systems (acoustic & condition monitors) deployed globally to detect wheel/track faults, showing industry adoption of sensing-based safety.
- **Academic sensor+ML works:** Machine learning applied for obstacle & crack detection on tracks using camera and IoT sensor data.
- **IoT-Enabled Railway Track Crack Detection System**: Presented at the International Conference on Innovative Computing & Communication, this research integrates IoT sensors along the track to detect cracks and anomalies in real time.

Github: https://github.com/thesurajarya/hack4delhi.git


IEEE NSUT


दिल्ली नगर निगम
MUNICIPAL CORPORATION OF DELHI
तमसो मा ज्योतिर्गमय


Delhi Transport Corporation


DEEN DAYAL UPADHYAYA
COLLEGE
UNIVERSITY OF DELHI


ज्योतिर्वृणीत तमसो विजानन्


आ नो भद्रा क्रतवो यन्तु विश्वतः
NSUT
NETAJI SUBHAS UNIVERSITY OF TECHNOLOGY

THANK YOU