IEEE NSUT

Delhi Transport Corporation

HACK4DELHI

Pitch Directly to the Government. Build for the Nation.

Team Name : !ordinary

Members name and Affiliation:

- Gaurav Yadav (NSUT)
- Arindam Shandilya (NSUT)
- Kashika Yadav (NSUT)
- Ridhima Aggarwal (NSUT)
- Yajat Suri (NSUT)

IEEE NSUT

PROBLEM STATEMENT

Domain 3, PS - 3

AI system to detect intentional railway track tampering.
An AI-based anomaly detection system to ensure public safety and infrastructure security.

Indian Railways is one of the largest and most heavily utilized transport networks in the world. In 2025 alone, over 693 crore (6.93 billion) passengers travelled by train, with an average of 2,300 lakh (23 million) people relying on railways every day. For students, laborers, daily-wage workers, families, and businesses, trains remain the only affordable and accessible mode of long-distance transportation.

India presents unique challenges that make track monitoring especially difficult. Railway track anomalies can arise from both natural causes and intentional tampering. Natural factors include temperature-based expansion and contraction between summer and winter, continuous train vibrations, and normal environmental variations. Intentional tampering involves deliberate loosening of fasteners, removal of track components, or placement of foreign objects.

In India, these risks are amplified by extremely high passenger density, limited resources for continuous manual inspection, and vast, diverse terrain spanning plains, mountains, deserts, and flood-prone regions. Additionally, overcrowding and unauthorized track crossings further increase infrastructure vulnerability. Recent news reports have also flagged multiple accidental fatalities involving both humans and wildlife, such as elephant deaths caused by accidental track crossings highlighting the urgent need for improved monitoring and early warning systems. Together, these factors make it difficult for existing systems to reliably distinguish natural variations from deliberate sabotage.

To address these challenges, we propose a machine intelligence driven system to detect and respond to intentional railway track tampering. This system is tailored to India’s unique conditions and aims to prevent disruptions, protect lives, and secure the integrity of the rail network.

IEEE NSUT

SOLUTION

To tackle the safety risks and operational issues faced by Indian Railways, we propose an AI-powered *railway track monitoring system* designed to spot deliberate track tampering in real-world Indian environments. The system keeps a constant watch on railway tracks using multiple sensors that record structural movement, vibrations, obstructions, and environmental data.

By understanding normal track behaviour in various seasons, terrains, and load conditions, the system can detect sudden, localised, and unusual changes that do not match natural wear or environmental differences. These changes indicate deliberate tampering or sabotage. Unlike traditional systems that rely on set thresholds, this method is aware of its context and adapts to factors like temperature changes, ongoing train vibrations, heavy axle loads, and regional differences. A risk-scoring mechanism ranks alerts based on severity, frequency, and pattern consistency. This helps ensure timely and appropriate responses, even with limited inspection resources. The solution is practical and scalable for a vast railway network. Overall, the system improves public safety, lowers derailment risks, reduces major service disruptions, and boosts national railway security through early detection and smart, data-driven decisions.

IEEE NSUT

ARCHITECTURE

Real-time, AI-driven tampering detection from track to dashboard

Data Flow (Horizontal Flow)

- Icons + Arrows Layout:
- Track - Mounted Sensors → Arduino Uno (Edge Device) → Python Ingestion & Preprocessing → AI Anomaly Detection Engine → Stream-lit Dashboard & Alerts

Sensing Layer

- Flex Sensor → Rail bending/loosening
- Ultrasonic → Gaps or obstacles
- PIR → Unauthorized (human or animal) presence
- Temperature → Environmental effects

Edge Layer

- Arduino Uno → Reads & streams sensor data
- Low-cost, scalable deployment

Data Processing Layer

- Python ingestion → Filtering, timestamping, feature extraction
- Structured for AI analysis

AI & Detection Layer

- Rule-based logic + ML (Isolation Forest, LOF)
- Detects anomalies → Assigns risk scores

Application Layer

- Stream-lit dashboard → Live sensor readings
- Alerts → Risk levels → Operator response

Key Characteristics (Icons + Keywords)

- Multi-sensor fusion → Reliable detection
- Context-aware AI → Adapts to temperature, load, vibration
- Real-time & scalable → Low-cost, practical for Indian railways

TECHNOLOGY USED

IEEE NSUT

Hardware (Simulated in TinkerCad)

- Arduino Uno – Sensor data acquisition
- Flex Sensor – Detects track bending or loosening
- Ultrasonic Sensor (HC-SR04) – Identifies gaps or foreign objects
- PIR Sensor – Detects unauthorized human presence
- TMP36 Temperature Sensor – Filters environmental heat vs cutting/welding activity

Software & Tools

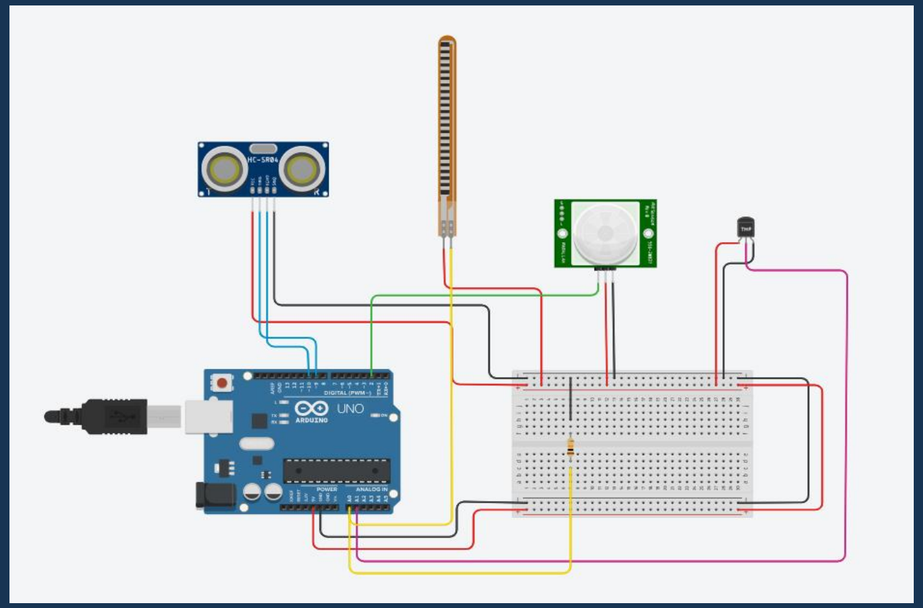
- Arduino IDE / TinkerCad – Circuit simulation & serial output
- Python – Data ingestion, preprocessing, and AI logic

Machine Learning Models

- Isolation Forest (global anomaly detection)
- Local Outlier Factor (localized tampering patterns)
- Stream-lit – Real-time dashboard and alert visualization

AI Approach

- No hard-coded rules
- Context-aware learning using multi-sensor correlations
- Differentiates natural variations from Intentional tampering

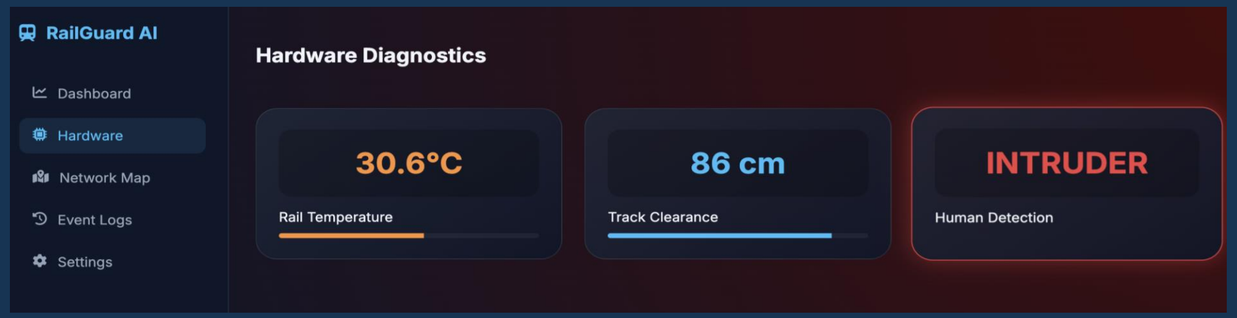


IEEE NSUT

FEATURE/USP

Unique Selling Points (USP)

- **Context-Aware Detection:**
  Distinguishes natural effects (temperature, vibration, load) from deliberate tampering
- **Multi-Sensor Fusion:**
  Human presence + structural strain + obstruction + heat = high-confidence detection
- **Unsupervised ML:**
  Works even without labeled sabotage data
- **Scalable & Cost-Effective:**
  Designed for vast, resource-constrained railway networks like India
- **Real-Time Alerts:**
  Enables faster response, reducing derailment and service disruption risks



Future Enhancements

- Deploy on **real hardware** (Raspberry Pi + live sensors)
- Integrate **CCTV and drone feeds** with computer vision
- Cloud deployment with **SMS/email alerting**
- Train **supervised ML models** using labeled incident data
- Integration with **railway control centers** for automated response

IEEE NSUT

REFERENCES/LINKS

- Github Repositary - Github
- RailGuardAI app - RailGuardAI
- Google Collab - GoogleColab
- Tinker-Cad - TinkerCad
- Video Demo - video

IEEE NSUT

Delhi Transport Corporation

THANK YOU