Regional IoT Forecasting: Advancing Time Series Analysis, Anomaly Detection, and Cybersecurity Using AI Models

Abstract

The exponential growth of IoT devices has generated vast amounts of time series data, creating opportunities to enhance human activities, ensure device reliability, and safeguard against cyber threats. This project integrates multiple research areas, focusing on time series forecasting, real-time anomaly detection, and cybersecurity. By utilizing the DDoS Botnet Attack on IoT Devices dataset and the IoT Telemetry Sensor Data Analysis dataset, this research employs transformer models and exploratory data analysis (EDA) to drive insights and optimize IoT ecosystem functionality within a given Region. Key deliverables include accurate environmental forecasting, robust anomaly detection mechanisms, and actionable insights for human activity optimization.

Dataset Details

1. **IoT Telemetry Sensor Data Analysis Dataset** :
    - Description: This dataset includes telemetry data capturing temperature, humidity, and pressure over time, ideal for time series forecasting and anomaly detection
    - https://www.kaggle.com/code/chaozhuang/iot-telemetry-sensor-data-analysis
2. **DDoS Botnet Attack on IoT Devices Dataset**:
    - Description: This dataset contains network traffic data from IoT devices operating under normal and DDoS attack scenarios, enabling the development of cybersecurity detection frameworks.
    - https://www.kaggle.com/datasets/siddharthm1698/ddos-botnet-attack-on-iot-devices

Research Areas

1. **Time Series Forecasting:**
    - Development of transformer-based models for predicting environmental parameters like temperature, humidity, and pressure.
2. **Human-Environment Interaction Optimization:**
    - Providing recommendations based on environmental telemetry to enhance human safety, comfort, and productivity.
3. **Anomaly Detection:**
    - Design of real-time systems to identify irregularities in IoT devices, including malfunctions and abnormal telemetry patterns.
4. **Cybersecurity for IoT Devices:**
    - Detection and mitigation of cyberattacks, such as DDoS attacks, targeting IoT infrastructures using network traffic analysis.
5. **Exploratory Data Analysis (EDA):**

    - Application of EDA to uncover patterns, relationships, and anomalies within IoT telemetry and network datasets.
6. **Predictive Maintenance:**
    - Early identification of potential IoT device failures, leveraging anomaly detection to enable predictive maintenance strategies.

Objectives

1. **Develop Transformer Models for Time Series Forecasting:**
    - Utilize advanced architectures to predict trends in environmental telemetry data.
    - Validate the models' superiority over traditional techniques in terms of accuracy and robustness.
2. **Optimize Environmental Insights for Human Activities:**
    - Analyze telemetry data to provide actionable insights for improving human interaction with the environment.
3. **Detect IoT Device Malfunctions:**
    - Create systems to identify early signs of device failures and recommend predictive maintenance.
4. **Identify and Mitigate Cyberattacks:**
    - Leverage network traffic data to build robust cybersecurity frameworks for detecting and countering cyber threats.

Methodology

1. **Data Preprocessing and EDA:**
    - Ensure data compatibility with machine learning workflows.
    - Explore datasets to identify patterns and initial anomalies.
2. **Model Development:**
    - Train and fine-tune transformer models for forecasting tasks.
    - Create anomaly detection systems using statistical and machine learning methods.
3. **Evaluation Metrics:**
    - Use metrics like MAE, RMSE, and F1-score to evaluate model performance.
    - Assess anomaly detection effectiveness through precision, recall, and detection latency.

Expected Outcomes

- Reliable forecasts for environmental parameters using transformer models.
- Real-time anomaly detection for identifying malfunctions and cybersecurity threats.
- Enhanced human-environment interactions through data-driven insights.