Zonal IoT Forecasting: Enhancing Time Series Analysis, Anomaly Detection, and Cybersecurity in IoT Systems

Abstract

The increasing proliferation of IoT devices generates extensive time series data, offering opportunities to enhance human activities, improve device reliability, and strengthen cybersecurity. This project leverages transformer models and exploratory data analysis (EDA) to advance time series forecasting, real-time anomaly detection, and cybersecurity measures. By utilizing the **IoT Telemetry Sensor Data Analysis** and **DDoS Botnet Attack on IoT Devices** datasets, the research aims to enhance IoT ecosystem performance within a defined region. Key outputs include an **interactive IoT dashboard for real-time insights**, a **comprehensive system design document**, and a **detailed proposal covering objectives, methodology, and anticipated outcomes**.

Dataset Overview

- **IoT Telemetry Dataset**: Logs temperature, humidity, and pressure variations collected via environmental sensors.
- **DDoS Botnet Dataset**: Records network traffic patterns to assess IoT-related cyber threats.
- **Size**: ~405K records in telemetry, ~7.5M records in the botnet dataset.

Research Areas

1. **Time Series Forecasting**: Leveraging transformer models for environmental trend prediction.
2. **Anomaly Detection**: Identifying unusual patterns in IoT sensor data.
3. **Cybersecurity**: Detecting and mitigating IoT-targeted cyber threats like DDoS attacks.
4. **Predictive Maintenance**: Proactively identifying IoT device malfunctions before failures occur.

Objectives

1. **Develop AI-based Forecasting Models**: Improve accuracy in predicting environmental conditions.

2. **Enhance Human-Environment Interaction**: Provide actionable insights based on IoT telemetry.
3. **Improve IoT System Reliability**: Implement early malfunction detection and preventive measures.
4. **Strengthen IoT Security**: Establish robust cybersecurity frameworks to counteract network-based threats.

Methodology

1. **Data Preprocessing & EDA**: Standardizing datasets and uncovering patterns.
2. **Model Training & Optimization**: Developing transformer-based forecasting and anomaly detection models.
3. **Performance Evaluation**: Using MAE, RMSE, and F1-score to assess model effectiveness.

Expected Outcomes

- **Reliable forecasting** for environmental monitoring.
- **Real-time detection** of IoT system failures and security breaches.
- **An intuitive IoT dashboard** for comprehensive data tracking and analysis.
- **A structured system architecture** for implementation and scalability.

IoT Application/System

This project proposes an **AI-driven IoT Monitoring System**, integrating:

- **Predictive analytics** to anticipate environmental variations.
- **Anomaly detection** to identify potential IoT failures and cyber threats.
- **A real-time IoT dashboard** for data visualization and alert notifications.

Industry Relevance & Target Users

- **Industries**: Smart Cities, Industrial IoT, Cybersecurity, Smart Homes.
- **Users**: IoT system administrators, urban planners, security analysts, and manufacturers.

References

1. Chao Zhuang. "IoT Telemetry Sensor Data Analysis." Kaggle, 2024. Link
2. Siddharth M. "DDoS Botnet Attack on IoT Devices Dataset." Kaggle, 2024. Link

3. Vaswani et al. "Attention Is All You Need." NeurIPS, 2017.