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

Abstract

The exponential growth of IoT devices has provided an abundance of time series data, providing 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. Utilizing the DDoS Botnet Attack on IoT Devices dataset and the IoT Telemetry Sensor Data Analysis dataset, this research applies transformer models and exploratory data analysis (EDA) to extract valuable insights and optimize IoT ecosystem functionality within a given region or zone. The project includes developing an interactive IoT dashboard for real-time visualization, a system design document for detailed architecture, and a comprehensive proposal outlining objectives, methodology, and expected outcomes.

Dataset and Application Proposal

Dataset Overview

Source of Dataset

This project utilizes two publicly available datasets from **Kaggle**:

1. **IoT Telemetry Sensor Data Analysis Dataset** - Contains sensor readings for environmental monitoring.
    - Link to dataset
2. **DDoS Botnet Attack on IoT Devices Dataset** - Captures network traffic data to study IoT-based cyberattacks.
    - Link to dataset

Data Collection Methods

- The **IoT Telemetry dataset** was collected using environmental sensors deployed across different locations to track temperature, humidity, and pressure variations over time.

- The **DDoS Botnet dataset** was gathered through controlled experiments simulating normal and attack scenarios on IoT devices to monitor network behavior and traffic patterns.

Number of Observations

- **IoT Telemetry dataset**: Contains **405,184 observations**.
- **DDoS Botnet dataset**: Includes **approximately 7.5 million network traffic logs**.

Variables in the Dataset

- **IoT Telemetry dataset**:
  - `timestamp` (time of data capture)
  - `temperature` (in Celsius)
  - `humidity` (percentage)
  - `pressure` (in hPa)
  - `device_id` (sensor identifier)
- **DDoS Botnet dataset**:
  - `timestamp` (network event time)
  - `src_ip` (source IP address)
  - `dst_ip` (destination IP address)
  - `protocol` (TCP, UDP, ICMP, etc.)
  - `attack_type` (benign or specific attack type)

IoT Application/System Design

Application Description

This project proposes an **AI-powered IoT Monitoring System** that integrates **predictive analytics, anomaly detection, and cybersecurity threat analysis**. The system will:

- **Monitor and forecast environmental conditions** using AI models.
- **Detect IoT device failures and cyber anomalies** using real-time data processing.
- **Provide a user-friendly IoT dashboard** to visualize sensor trends and security alerts.

Target Users

- **Industrial IoT operators** for predictive maintenance.
- **Smart city infrastructure planners** for environmental monitoring.
- **Cybersecurity teams** to detect and mitigate IoT-based attacks.
- **IoT device manufacturers** for reliability assessments.

Industry Fit

The IoT application fits into multiple industries:

- **Smart Cities** – Real-time environmental tracking and anomaly alerts.
- **Industrial IoT (IIoT)** – Predictive maintenance of sensors and devices.
- **Cybersecurity** – Protection against IoT-targeted cyberattacks.
- **Smart Homes** – Monitoring temperature and humidity variations to optimize Heating, Ventilation, and Air Conditioning systems.

Methodology

1. **Data Preprocessing and EDA**
    - Cleaning, normalizing, and structuring IoT telemetry and network logs.
2. **Model Development**
    - Implementing **transformer-based forecasting** for sensor trends.
    - Developing **machine learning-based anomaly detection** for IoT security.
3. **IoT Dashboard Development**
    - Real-time visualization using **Tableau.**
4. **System Documentation**
    - Writing a **detailed system design document** for technical implementation.

Expected Outcomes

- **Accurate forecasting of environmental conditions** using AI models.
- **Real-time alerts for IoT malfunctions and cyberattacks**.
- **User-friendly IoT dashboard for live data tracking**.
- **Comprehensive system design documentation** for deployment.

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.