Proposal: Zonal IoT Forecasting - Enhancing Time Series Analysis, Anomaly Detection, and Cybersecurity

Abstract

The proliferation of IoT devices generates vast amounts of **time-series data**, presenting opportunities for **predictive analytics, anomaly detection, and cybersecurity improvements**. This project utilizes **machine learning (ML) and transformer-based models** to enhance **IoT forecasting, real-time anomaly detection, and security monitoring**. We leverage two datasets: **IoT Telemetry Sensor Data Analysis** (capturing temperature, humidity, and pressure) and **DDoS Botnet Attack on IoT Devices** (analyzing network traffic for cyber threats). The research focuses on **time series forecasting, predictive maintenance, and AI-driven intrusion detection systems (IDS)**. The anticipated outcomes include an **AI-powered IoT monitoring dashboard**, accurate forecasting models, and improved security frameworks for IoT ecosystems.

Dataset Overview

1. Source & Data Collection

- **IoT Telemetry Sensor Data:** Collected from **environmental sensors** tracking temperature, humidity, and pressure.
- **DDoS Botnet Attack Dataset (BoTNeTIoT-L01):** Captured using **Wireshark** from **nine IoT devices**, logging both **normal and attack traffic**.

2. Dataset Size & Variables

- **IoT Telemetry Dataset: ~405,000 observations**, logging environmental variations.
- **DDoS Botnet Dataset: ~7.5 million observations**, with **23 engineered features** (e.g., packet count, jitter, network traffic patterns).
- **Key Variables:** Temperature, humidity, pressure, packet size, attack classification, network latency, and device activity logs.

Research Points

This project focuses on **four core areas**:

1. Time Series Forecasting (Transformers & ML)

- Utilize **transformer-based models (e.g., Temporal Fusion Transformers, LSTMs)** to predict **IoT environmental trends** (temperature, humidity).
- Improve **IoT reliability** by forecasting conditions affecting device performance.

2. Real-Time Anomaly Detection

- Implement **unsupervised ML models** (Autoencoders, Isolation Forests) to detect **anomalies in IoT telemetry and network traffic**.
- Develop a **predictive maintenance system** to identify **device failures before they occur**.

3. IoT Cybersecurity & DDoS Threat Detection

- Apply **deep learning-based intrusion detection systems (IDS)** to **analyze botnet attacks** in IoT traffic.
- Enhance **IoT network security** against **DDoS threats like Mirai and Gafgyt**.

4. AI-Powered IoT Monitoring Dashboard

- Integrate an **interactive dashboard** for real-time tracking, **visualizing trends, anomalies, and security threats**.
- Provide **actionable alerts** to **IoT administrators, security analysts, and industrial operators**.

IoT Application & Industry Relevance

- **Application: AI-driven IoT monitoring system** for **predictive analytics, security monitoring, and anomaly detection**.
- **Users: Smart city operators, industrial IoT engineers, cybersecurity analysts, and home automation developers**.
- **Industry Fit: Smart Cities, Industrial IoT, Cybersecurity, Smart Homes**.

Expected Outcomes

Improved time series forecasting using transformers.
Real-time anomaly detection for IoT system failures.
AI-powered IDS to detect cyber threats.
Interactive IoT dashboard for monitoring and alerts.
Scalable IoT security framework for industrial & smart city applications.

By integrating **AI, ML, and cybersecurity solutions**, this project aims to **enhance IoT resilience, reliability, and security**, supporting **smarter, safer connected environments**.