Title : Convergence of IoT, machine learning, and advanced analytics to address critical challenges in forecasting, anomaly detection, and cybersecurity.

Abstract

The rapid expansion of IoT devices generates massive volumes of time-series data, creating opportunities for predictive analytics, anomaly detection, and cybersecurity enhancements. This project leverages machine learning (ML) and transformer-based models to refine IoT forecasting, enable real-time anomaly detection, and strengthen security monitoring. Two datasets are utilized: **IoT Telemetry Sensor Data Analysis** (tracking temperature, humidity, and pressure) and **DDoS Botnet Attack on IoT Devices** (examining network traffic for cyber threats). The research primarily focuses on time series forecasting, predictive maintenance, and AI-driven intrusion detection systems (IDS). Expected outcomes include an AI-powered IoT monitoring dashboard, precise forecasting models, and enhanced security frameworks for IoT ecosystems.

Dataset Overview

1. Source & Data Collection

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

2. Dataset Size & Key Variables

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

Research Focus Areas

1. Time Series Forecasting (Transformers & ML)

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

2. Real-Time Anomaly Detection

- Deploy unsupervised ML models (**Autoencoders, Isolation Forests**) to detect anomalies in IoT telemetry data.

3. IoT Cybersecurity & DDoS Threat Detection

- Implement deep learning-based **intrusion detection systems (IDS)** to analyze botnet attacks in IoT network traffic.
- Strengthen IoT network security against DDoS threats such as **Mirai** and **Gafgyt**.

4. AI-Powered IoT Monitoring Dashboard

- Develop an interactive dashboard for real-time tracking, visualizing trends, and identifying anomalies.

IoT Applications & Industry Relevance

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

Expected Outcomes

- **Enhanced time series forecasting** using transformer-based models.
- **Real-time anomaly detection** for IoT system failures.
- **AI-powered intrusion detection systems (IDS)** for identifying cyber threats.
- **Interactive IoT monitoring dashboard** for tracking and alerts.
- **Scalable IoT security framework** applicable to industrial and smart city environments.

By integrating AI, ML, and cybersecurity technologies, this project aims to improve the resilience, reliability, and security of IoT systems, fostering smarter and more secure connected environments.

References

[1] A. Alhowaide, I. Alsmadi, J. Tang. “Towards the design of real-time autonomous IoT NIDS”, *Cluster Computing* (2021), pages 1-14, Jan 2021.
[2] A. Alhowaide, I. Alsmadi, J. Tang, “Features Quality Impact on Cyber Physical Security Systems”, *2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, Oct. 2019.

Dataset Sources:

- IoT Intrusion Detection Dataset
- IoT Telemetry Sensor Data