Securing the Unseen: Real-Time IoT Device Security Monitoring

Real-Time Threat Detection and Response System for IoT Environments.

SK by Satyam Kumar

Introduction

Rapid IoT Growth

Billions of connected devices across homes, industries, and smart cities.

Security Implications

Many devices lack robust security due to limited computational power , cost saving measures and flawed design.

Current Gap

Traditional security tools aren't optimized for the unique characteristics of IoT environments.

Problem Statement

Unauthorized Access

Using default or weak credentials.

Malware Infections

Botnets like Mirai target IoT devices.

Sensitive Data Leaks

Insecure communications expose data.

DDoS attacks

leveraging compromised devices.

Project Objective

1

Lightweight System

Efficient and scalable IoT monitoring.

2

Continuous Monitoring

Monitor network and device behavior.

3

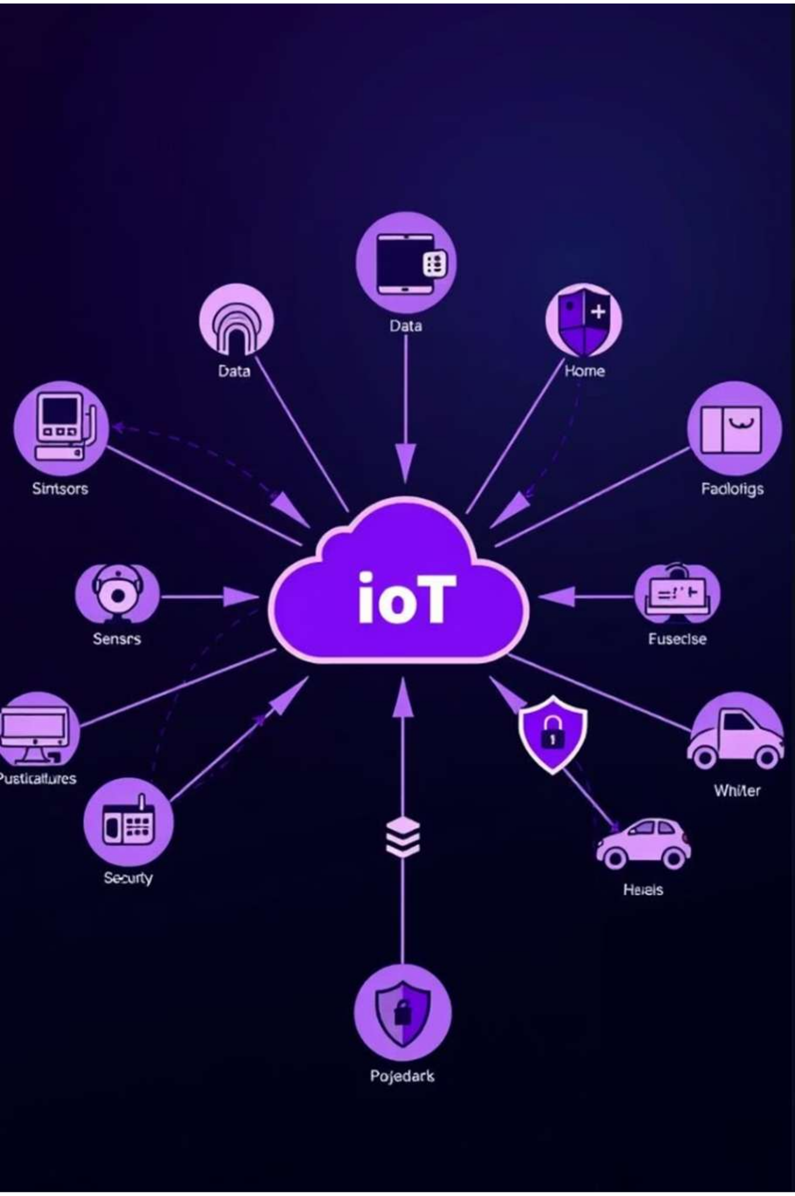
Real-Time Alerts

Automated mitigation of threats.

4

Protocol-aware

and modular system design



System Architecture

IoT Devices

sensors, cameras, smart gadgets

Passive Sniffers

E.g. Zeek, Tcpdump

Central Monitoring Server

Runs monitoring software like Nagios, Zabbix .

Visual Dashboard

Grafana, Kibana

Anomaly Detection Engine:

ML-based detection scikit-learn, TensorFlow

Alerting & Mitigation Module

Notifies the security admin for further investigation.

Key Features

Real-time traffic inspection and analysis

ML-driven anomaly detection

Signature-based threat identification

Alert notifications (email, SMS, webhook)

Automated response actions:

- Device isolation
- Traffic throttling or blocking
- Admin notifications

Technologies Used

Languages

Python, Node.js, HTML , CSS, JavaScript

Network Tools

Zeek , Suricata, tcpdump ,WireShark.

Machine Learning

scikit-learn, TensorFlow, Isolation Forest, K-Means.

Supported Protocols

MQTT, CoAP, HTTP, Zigbee, UPnP

Anomaly Detection Logic

1

Normal Behavior Modeling:

Learn traffic patterns from baseline data.

2

Analyze Features:

Packet rate and size.

Protocol usage.

Source and destination IP/Ports.

Payload variations.

3

Detections Techniques:

Isolation Forest, K-Means.

Custom rules for specific threats (e.g., DNS misuse).

Real-Time Response Module

Automated Actions:

Isolate devices via VLAN or firewall

Block or rate-limit suspicious IPs

Forward incident reports to SIEM

Admin Interface:

Real-time alerts via email, GUI, or mobile app

Detailed logs of actions taken for auditability

Dashboard & Visualization

Centralized GUI

Real-time device and traffic status.

Anomaly detection heatmaps and scores.

Alert history and trend timelines.

Tools Used

Grafana panels, Kibana dashboards

ELK filtering.

Bonus Capabilities

Firewall Integration

iptables, pf Sense

Supports diverse IoT protocols:

Zigbee, CoAP, UPnP, BLE

Lightweight Agent

Efficient support for edge devices.

Remote device

control and OTA firmware updates

Push notifications

for critical threat alerts

Real-World Applications

Smart Homes

Detect compromised smart TVs or locks.

Smart Cities:

Monitor traffic systems, public Wi-Fi routers, and surveillance cameras.

Industrial IoT

Secure SCADA systems and PLCs.

Future Enhancements

1

Blockchain Authentication

Ensure tamper-proof device identity.

2

Federated Learning

Train ML models without sharing raw data.

3

Threat Intelligence Feeds

Integrate with sources like AlienVault OTX.

Conclusion

Critical Blind Spot

Addresses a key gap in IoT cybersecurity.

Proactive Threat Detection

Real-time monitoring ensures defense.

Scalable and Adaptable

Suits a wide range of IoT ecosystems.

Enhances the resilience of modern, connected infrastructures

Q&A

Thank you for your attention.

Questions or feedback are welcome!