Analysis Report for IoT Intrusion Detection System (IDS)

CMPE 491

Ahmad Ismail 99000332006
Ateş Öztürk 21145665572
Esra Gürgen 40654688056

1. Introduction

This document gives a thorough check of the Intrusion Detection System (IDS) project, which is specially made for IoT devices. It also presents an official contract between those who develop and their client. We describe here what we hope to achieve with the project, what's expected from it and everyone's tasks involved so that all have clear expectations. Also, within this, we look closely at any worries or doubts that might arise to make sure there are no misunderstandings among team developers and others invested in the work done.

For this project, the main objective is to create a strong, expandable and smart security solution that is particularly for IoT environments. The prevalent use of IoT devices in different sectors like healthcare, intelligent homes, industrial automation and transportation has emphasized cybersecurity necessity in these areas. Because usual cybersecurity ways do not properly cover the special security dangers of IoT devices, our project plans to fill these voids by applying machine learning methods; both supervised and unsupervised learning are considered for fast and precise cyber threat detection. IDS has the goal to make sure IoT networks operate smoothly by immediately responding to threats. If a threat is noticed, the system starts quick response processes so as not to allow damage spread. This makes certain that uninterrupted working of IoT devices continue while keeping network security at high levels.

2. Current System

In this project range, no specific system for detecting intrusions is assigned to IoT environments. At present, companies use simple network security actions like firewalls, usual antivirus programs and manual supervision ways. However, these techniques are not enough against advanced and changing risks towards IoT networks. So, there is requirement for a specific IDS that has instant monitoring, adaptive detection and automated response abilities.

3. Proposed System

3.1 Overview

The Intrusion Detection System (IDS) is a highly developed cybersecurity tool. It's intentionally built for IoT settings. This system incorporates an array of top-notch machine learning techniques, like supervised learning to spot known threats and unsupervised learning for identifying anomalies. The goal of this framework is to provide all-inclusive and constant real-time network observation, with the mean purpose of recognizing potential dangers thus stopping them before they cause severe damage.

This system provides comprehensive protection by supporting many IoT communication protocols such as MQTT, CoAP, HTTP, Zigbee and Bluetooth. When a threat is detected, the system prevents the spread of damage by activating rapid response mechanisms. In this way, it maintains network security at a high level by ensuring the uninterrupted operation of IoT devices. In addition, it includes automatic event management mechanisms and offers measures such as instant alerts, IP address blocking and quarantine of compromised devices.

IDS possess an interface which is very intuitive, letting administrators use it with ease even without much training in cybersecurity. The system has been structured to be scalable and can adjust effectively to various network sizes as well as complexities. It also works well on IoT devices with limited resources. Furthermore, it strictly adheres to international data protection rules and cyber security standards like GDPR and NIST, which enhance the system's reliability and reputation.

To sum up, the suggested IDS shows a big improvement compared to old security systems. It gives smart, strong and easy-to-use answers for defending IoT surroundings from changing cyber dangers. So, by this method, IoT networks get more safety and managing security becomes quite simpler.

3.2 Functional Requirements

I. Real-time Network Monitoring: IoT network traffic will be continuously monitored, and suspicious activities will be detected instantly to ensure network security. In this process, potential threats in the network will be detected instantly using advanced analysis methods and each detection will be processed quickly to minimize the delay between detection and response. This will ensure that threats are eliminated quickly, especially in time-critical situations.

II. Advanced Intrusion Detection: Supervised machine learning algorithms performed on network traffic will compare with a constantly expanding and updated threat database to accurately detect known threats. At the same time, unsupervised learning algorithms and anomaly detection methods will analyze unusual changes in network traffic to recognize previously unseen or unknown threats. Thus, it identifies potential new threats at an early stage.

III. Automated Incident Management: When threats are recognized, safety actions will start automatically. These steps involve instant alerts to the administrators of networks, blockage of dubious device IP addresses and separation from network for endangered devices. These automatic actions will be done fast to stop situations from getting worse and to prevent the damage from spreading. This is useful for keeping a possible security risk under control before it turns into a significant issue.

IV. Protocol Compatibility: Various protocols will be backed up to make sure the security of IoT networks allows us to supervise different IoT tools and communication structures. The protocols we support include the usual IoT communication ones like MQTT, CoAP, HTTP, Zigbee and Bluetooth. There is also compatibility that helps in observing all kinds of devices and communication setups within network. This way it becomes easy for managing any sort of security dangers that might come up during communications on various types or kinds of devices and procedures effectively.

V. Integrated Security Management: The system will be designed to seamlessly integrate with existing IoT security infrastructure. This integration will strengthen overall network security and make threat management more effective. It will also work faster and more efficiently in the incident response process, ensuring that security breaches are detected in advance and that action is taken quickly.

VI. User-Friendly Interface: The system will provide a user-friendly graphical user interface where network security status, threat alerts and system configurations can be clearly displayed. This interface will be designed to allow users who do not have extensive cybersecurity knowledge to easily use the system. Thus, the management and monitoring of the system will be accessible and understandable even for users with different levels of technical knowledge.

VII. Comprehensive Reporting and Analytics: The system will be able to generate detailed reports and visual analysis on security events, threat patterns and response activities. These reports will help decision makers to determine security strategies more consciously. It will also enable them to take proactive steps for future security improvements. At the same time, all data related to network security will be analyzed collectively, creating a more efficient threat management process.

3.3 Nonfunctional Requirements

I. Performance: It is necessary to ensure that network traffic is processed quickly, and threats are detected efficiently. This will require optimizing system performance even under high traffic volumes and minimizing latency. The system must operate quickly and efficiently while handling high traffic volumes.

II. Accuracy and Reliability: Threat detection results will always be accurate, and the number of false positives and false negatives will be greatly reduced. For this purpose, continuous learning and system improvement processes will be implemented to increase the accuracy of detected threats and ensure reliability.

III. Scalability: The architecture of the system will be made such that it can easily scale as more and varied IoT devices are added. This means, when the network size grows larger, expanding the system won't harm its performance or security in any way. Further to this, we plan to support system development by including newer device types and protocols.

IV. Security and Compliance: We will use powerful codes for encrypting and safe communication methods to safeguard sensitive information. Also, we will make certain compliance with global cybersecurity standards such as GDPR, NIST etcetera. This will enhance the safety of data while also making sure that the structure is consistent with worldwide legal requirements.

V. Usability: The aim will be to develop an intuitive and accessible interface for users. This interface will enable users with different levels of technical knowledge to easily operate and manage the system. Thus, the need for users to receive training on the system will be minimized.

VI. Maintainability: System will be structured in simple way for updates, debugging and maintenance purposes. This makes it easy to develop the system's functions and quickly fix any issues that can occur. In addition, improvements to increase the system's performance will be easily integrated.

VII. Availability: High availability and fault tolerance will be provided. For this purpose, backup systems and redundancy mechanisms will be included. In this way, security monitoring will be carried out without interruption. In case of system failures, rapid recovery will be provided and there will be no disruption in the security monitoring process.

3.4 Pseudo Requirements

I. Cost-Effectiveness: Development and operational costs will be optimized by using open-source technologies. However, during this process, the performance and reliability of the system will be kept at a high level. A quality solution will be offered without compromising on costs.

II. Energy Efficiency: The system will be designed around low energy consumption. This will aim to provide optimal functionality in low-power IoT environments and extend the operational life of battery-powered IoT devices.

III. Ethical Transparency: Complete transparency will be ensured in the processes of data collection, processing and storage. All data processing activities will be shared with users. User trust and legal compliance will be protected by complying with ethical standards.

3.5 System Models

3.5.1 Scenarios

- **Scenario 1: Malware Detection**

    - **Description:** An IoT sensor device within a manufacturing plant is infected with malware. This malware initiates unusual data transmission patterns, sending large amounts of data at irregular intervals.

    - **System Action:** IDS (Intrusion Detection System) quickly identifies these irregular transmission patterns with algorithms used to detect anomalies. An alert is quickly sent to network administrators. The affected device is isolated from the network and a detailed record of the incident is kept for forensic analysis.

- **Scenario 2: Unauthorized Access Attempt**

    - **Description:** An unauthorized IoT device attempts to connect to the company's secure network and access sensitive data.

    - **System Action:** IDS instantly recognizes an unauthorized device and blocks the IP address of that device since it fails authentication checks. Network access is blocked, real-time notifications are sent to administrators. An incident report is created that includes the device's IP address, location, and attempted actions.

- **Scenario 3: Data Exfiltration Prevention**

    - **Description:** An IoT security camera sends abnormal outgoing data traffic to an external IP address, indicating an attempt at data theft.

    - **System Action:** After detecting abnormal outgoing data traffic, IDS automatically blocks the suspicious external IP. The compromised camera is quarantined. High priority alerts are sent to administrators. Additionally, additional scanning procedures are initiated to ensure that other network devices are not affected.

- **Scenario 4: Protocol Anomaly Detection**

    - **Description:** An IoT device that usually communicates with the MQTT protocol unexpectedly starts using the HTTP protocol.

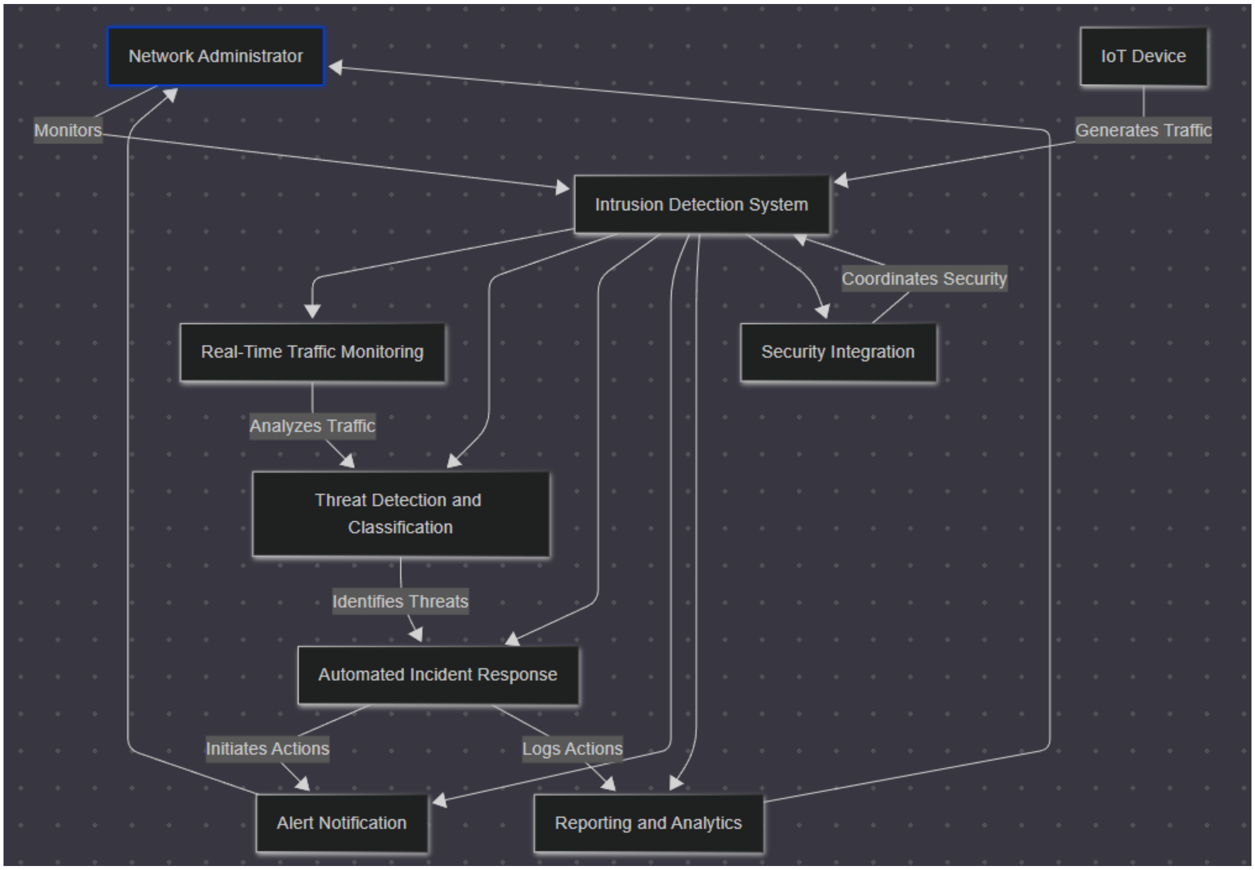
    - **System Action:** IDS immediately detects this protocol anomaly. It then generates an alert indicating the detected anomaly. The network access of the device is temporarily restricted for verification by an administrator or further investigation.

- **Scenario 5: Device Hijacking**

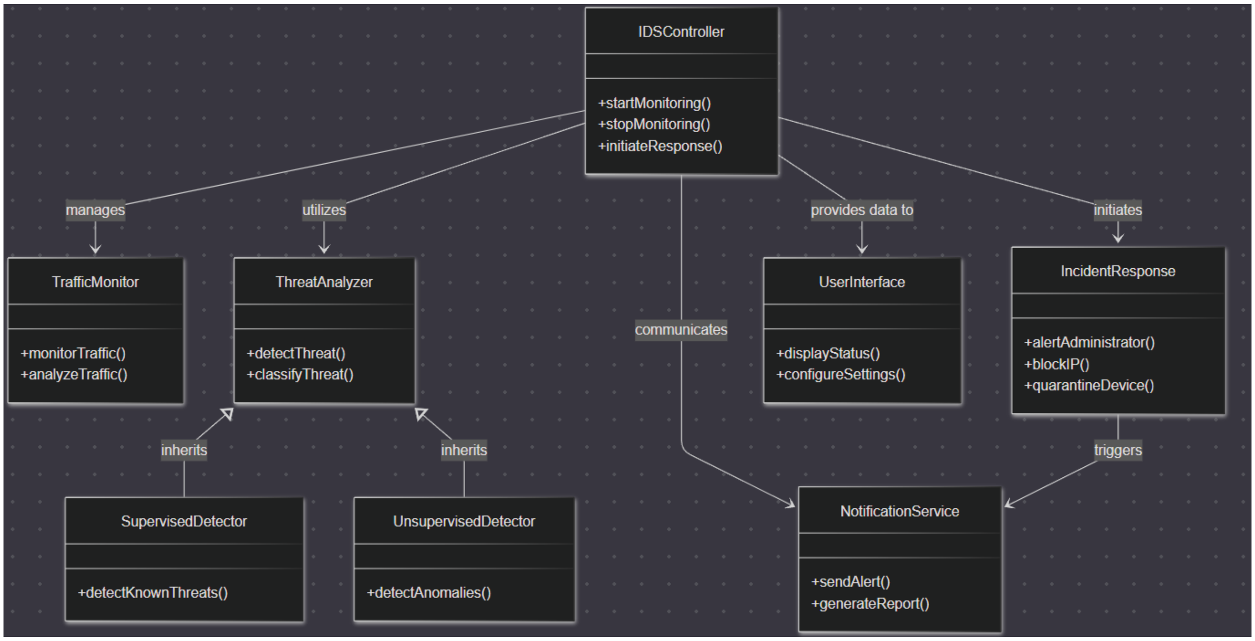
    - **Description:** An attacker significantly changes the operating parameters of the device by hijacking a smart thermostat.

    - **System Action:** IDS recognizes rapid configuration changes beyond certain thresholds, then triggers automatic security responses. The thermostat is isolated, secure default settings are restored, network administrators are immediately notified, and full details of the incident are recorded for an in-depth security review.

3.5.2 Use Case Model

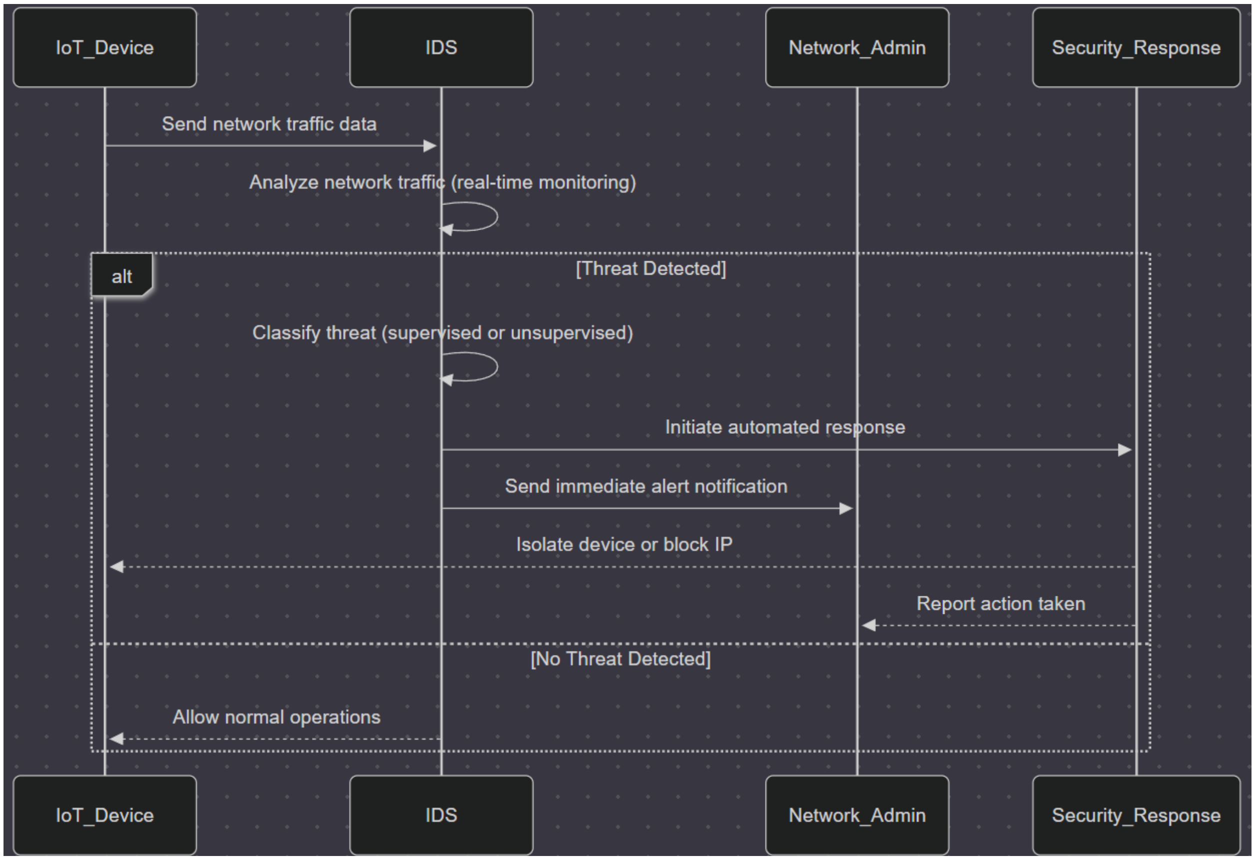


3.5.3 Object and Class Model

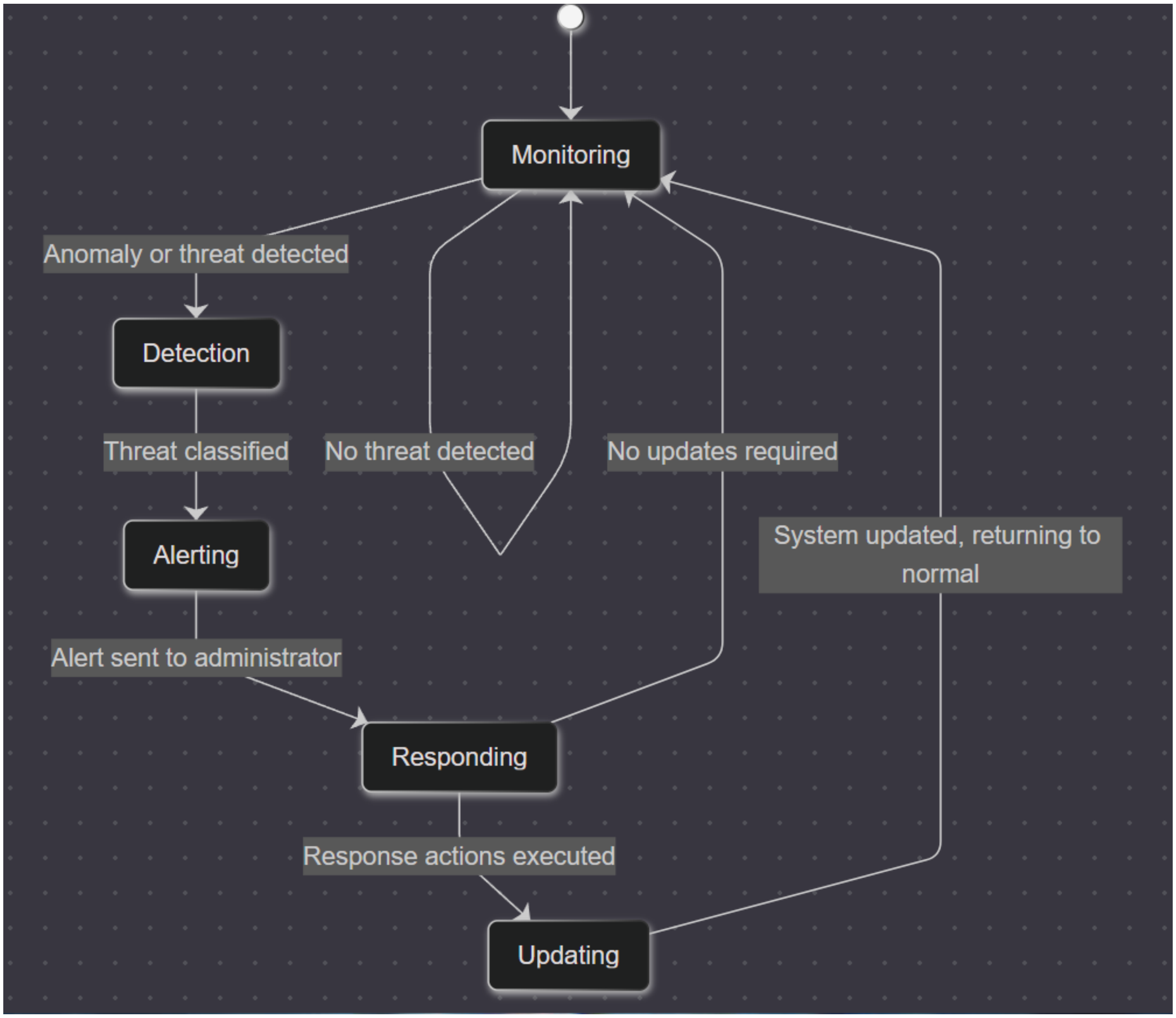


3.5.4 Dynamic Models

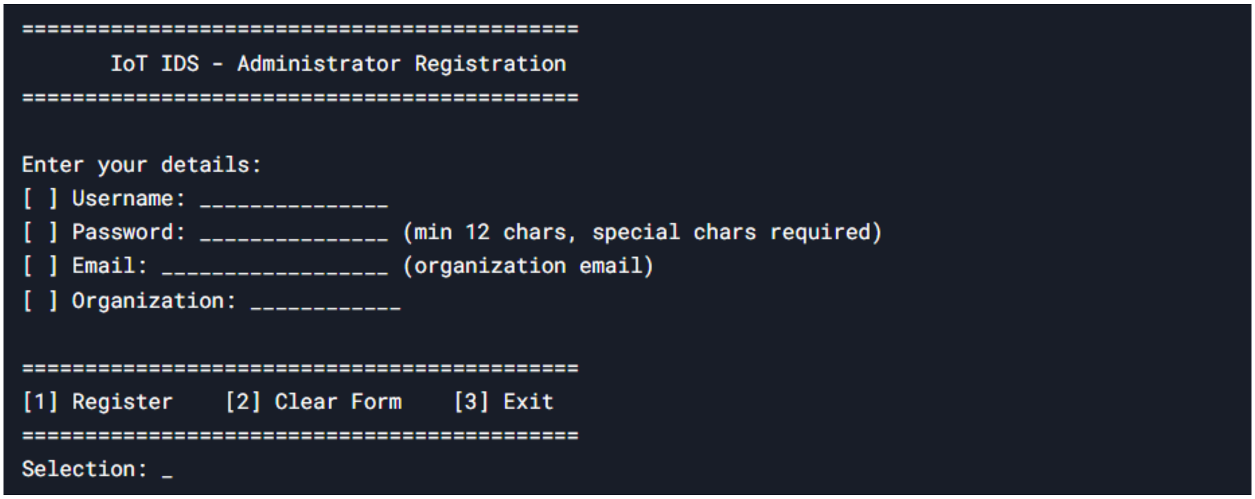
Sequence Diagram:


IoT_Device
IDS
Network_Admin
Security_Response
Send network traffic data
Analyze network traffic (real-time monitoring)
alt
[Threat Detected]
Classify threat (supervised or unsupervised)
Initiate automated response
Send immediate alert notification
Isolate device or block IP
Report action taken
[No Threat Detected]
Allow normal operations
IoT_Device
IDS
Network_Admin
Security_Response

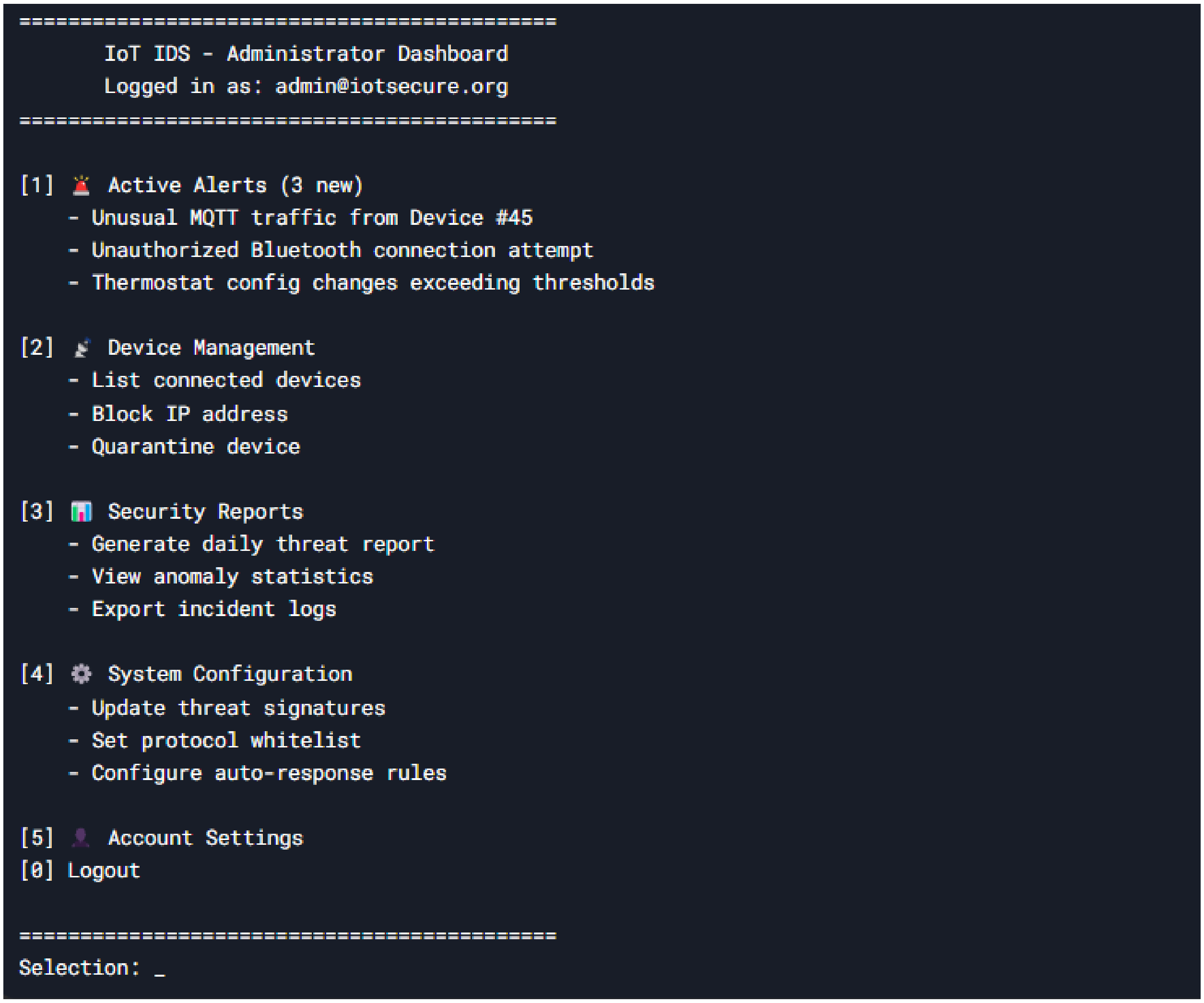
State Diagram:


Monitoring
Anomaly or threat detected
Detection
Threat classified
No threat detected
No updates required
Alerting
System updated, returning to normal
Alert sent to administrator
Responding
Response actions executed
Updating

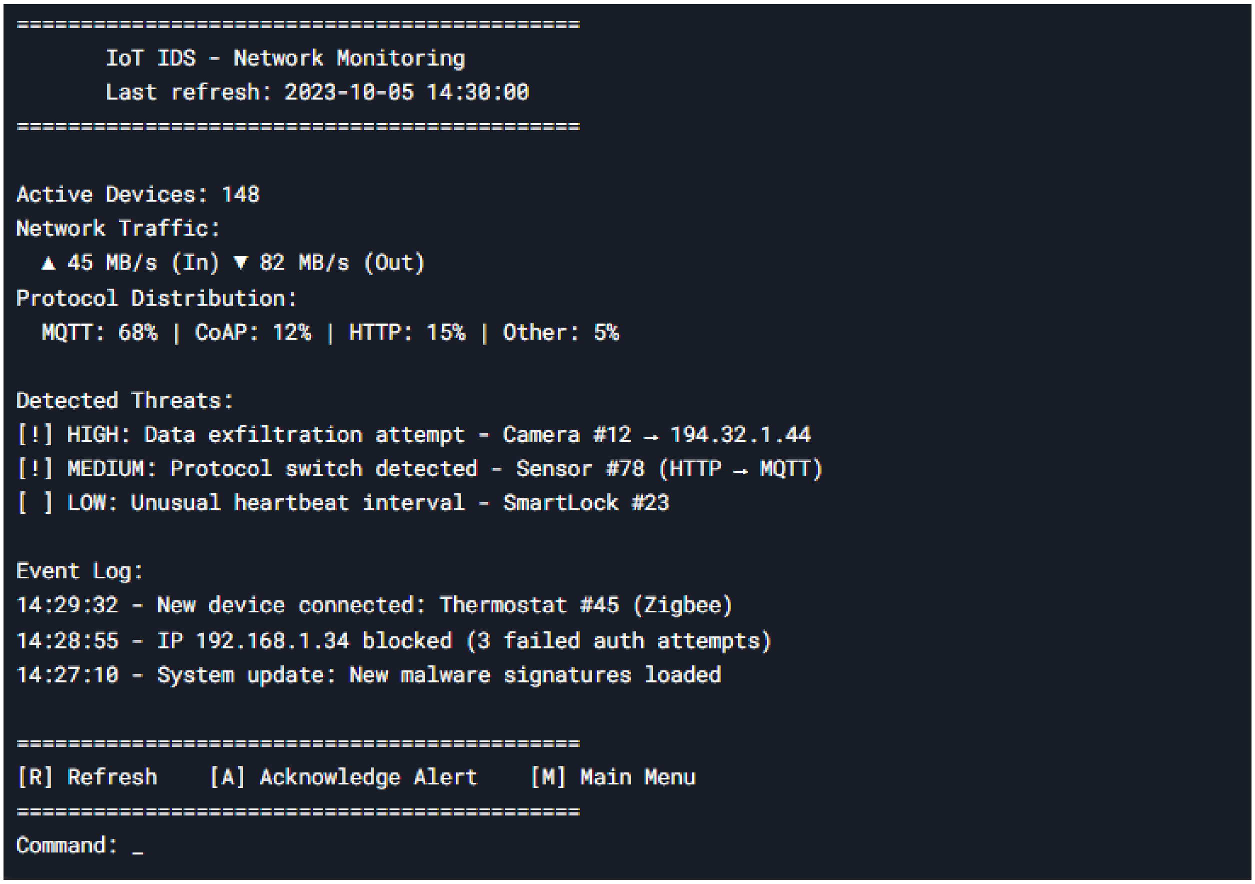
3.5.5 User interface - navigational paths and screen mock-up



```
============================================
       IoT IDS - Administrator Registration
============================================

Enter your details:
[ ] Username: _______________
[ ] Password: _______________ (min 12 chars, special chars required)
[ ] Email: __________________ (organization email)
[ ] Organization: ____________

============================================
[1] Register    [2] Clear Form    [3] Exit
============================================
Selection: _
```



```
============================================
       IoT IDS - Administrator Dashboard
       Logged in as: admin@iotsecure.org
============================================

[1] 🚨 Active Alerts (3 new)
    - Unusual MQTT traffic from Device #45
    - Unauthorized Bluetooth connection attempt
    - Thermostat config changes exceeding thresholds

[2] 📡 Device Management
    - List connected devices
    - Block IP address
    - Quarantine device

[3] 📊 Security Reports
    - Generate daily threat report
    - View anomaly statistics
    - Export incident logs

[4] ⚙ System Configuration
    - Update threat signatures
    - Set protocol whitelist
    - Configure auto-response rules

[5] 👤 Account Settings
[0] Logout

============================================
Selection: _
```



```
============================================
       IoT IDS - Network Monitoring
       Last refresh: 2023-10-05 14:30:00
============================================

Active Devices: 148
Network Traffic:
  ▲ 45 MB/s (In) ▼ 82 MB/s (Out)
Protocol Distribution:
  MQTT: 68% | CoAP: 12% | HTTP: 15% | Other: 5%

Detected Threats:
[!] HIGH: Data exfiltration attempt - Camera #12 → 194.32.1.44
[!] MEDIUM: Protocol switch detected - Sensor #78 (HTTP → MQTT)
[ ] LOW: Unusual heartbeat interval - SmartLock #23

Event Log:
14:29:32 - New device connected: Thermostat #45 (Zigbee)
14:28:55 - IP 192.168.1.34 blocked (3 failed auth attempts)
14:27:10 - System update: New malware signatures loaded

============================================
[R] Refresh    [A] Acknowledge Alert    [M] Main Menu
============================================
Command: _
```

4. Glossary

- **IDS (Intrusion Detection System):** It is a security system designed to continuously monitor network traffic and detect unauthorized access attempts or anomalies. This system quickly detects suspicious activities and notifies administrators. Thus, the security of the network is ensured. IDS helps prevent attacks by detecting potential threats in the network at an early stage.

- **IoT (Internet of Things):** It is a network system where physical devices are connected to each other via the Internet, collecting and sharing data. These devices are equipped with features such as sensors, software and network connectivity. They collect data from their environment, share this data with other devices and interact with each other.

- **Supervised Learning:** It is a machine learning method that allows algorithms to make accurate predictions. It uses labeled datasets. In this method, the model is trained with correctly labeled data, and the model is taught with the given data to predict a specific output.

- **Unsupervised Learning:** This machine learning method works with unlabeled data. The model focuses on discovering hidden patterns or anomalies in the data. Unsupervised learning is especially used to detect unknown threats and understand the natural relationship between data sets.

- **Anomaly Detection:** The detection of unusual patterns or behaviors in data. This technique is used to detect security threats or system errors at an early stage. For example, it identifies situations where a device is sending an amount of data it normally would not or generating network traffic at unusual hours.

- **False Positive:** A situation where a system incorrectly identifies a harmless situation as a threat. A security measure or detection system incorrectly flags behavior as malicious when it is not actually a threat. This can cause unnecessary alarms and actions.

- **False Negative:** It is the situation where a real threat or security breach is not detected by the system. Although there is a threat, the security software ignores it and the threat remains active.

- **Quarantine:** It is the isolation of a device after it is detected as a security threat in order to prevent it from affecting other devices on the network. The quarantined device is kept outside the network and is re-introduced to the system after its security is ensured.

- **MQTT, CoAP, HTTP, Zigbee, Bluetooth:** There are various communication protocols used for IoT devices to communicate with each other. Each protocol offers different advantages according to different application requirements.

- **GDPR (General Data Protection Regulation):** It is a legal framework enacted by the European Union and aims to protect personal data. This regulation regulates the collection, processing and storage of personal information of individuals and requires that this data be protected securely.

- **NIST (National Institute of Standards and Technology):** It is a U.S. government agency that develops standards and guidelines in the field of cybersecurity and technology. NIST provides guidance for security policies, encryption techniques, threat detection methods, and other security measures.

5. References

1. NIST Cybersecurity Framework - https://www.nist.gov/cyberframework

2. IEEE Cybersecurity Standards - https://www.ieee.org/about/corporate/governance/ethics.html

3. GDPR Compliance Guidelines - https://gdpr.eu/