Project Specifications Report

CMPE 491

Ahmad Ismail 99000332006
Ateş Öztürk 21145665572
Esra Gürgen 40654688056

1. Introduction

1.1 Overall Goal

The goal of this project is to create an Intrusion Detection System (IDS) for IoT devices. This system will improve network security, spot harmful activities and prevent possible dangers in immediate time. The IDS will use machine learning and unusual detection methods to keep check on network traffic, recognize patterns and find intrusions.

The project aims to create a scalable and adaptive IDS that ensures minimal false positives while providing automated responses to detected intrusions. The system will integrate supervised and unsupervised learning algorithms to detect known and unknown threats, ultimately improving the overall security of IoT networks.

1.2 Expected Outcomes

- **Accurate Intrusion Detection:** Development of an AI driven system that can effectively detect security threats in IoT environments.
- **Real Time Monitoring:** Continuous monitoring of network traffic for anomaly detection.
- **Low False Positives**: Optimizing machine learning models to decrease unnecessary alerts and false alarms.
- **Scalability:** To ensure the IDS can adapt to varying IoT network sizes and configurations.
- **User Friendly Interface:** A system that needs no elaborate preparation and can be easily controlled and maintained without professional knowledge, so that it can be easily combined with current network architecture**.**
- **Automated Incident Response:** Countermeasures including alert notifications, traffic filtering, and potential quarantine of compromised devices are implemented.

1.3 Constraints

The development and deployment of the IDS system must account for several constraints, including:

- **Economic Constraints:** The system should be cost-effective and should try to use open-source libraries to the highest possible level without compromising on performance.

- **Environmental Constraints:** The energy consumption of the AI based intrusion detection system should be minimized to make it suitable for low power IoT devices.
- **Social Constraints:** The system should be designed to preserve users' privacy and at the same time meet legal requirements such as GDPR.
- **Political Constraints:** This paper aims to ensure that the system is compliant with national and international cybersecurity standards and regulations to avoid legal issues
- **Ethical Constraints:** The IDS should not disrupt normal network operations and should be completely transparent with no hidden data collection.
- **Health & Safety Constraints:** The system should not create back doors that can be exploited to make the IoT-based healthcare or industrial control systems unsafe.
- **Manufacturability Constraints:** The solution should be portable to all kinds of IoT architecture and should be easily embedded into current security architectures.
- **Sustainability Constraints:** The IDS should be developed to work efficiently with little or no hardware enhancement and maintenance.

1.4 Professional and Ethical Issues

Designing and implementing an IDS system implies several professional and ethical commitments:

- **Data Privacy and Security**: The system must meet the legal requirements for data collection and processing (e.g., GDPR, NIST standards), as well as avoid leakage of user's data.
- **Transparency and Accountability**: AI-based decision making for detection should be understandable to avoid bias in the classification process.
- **User Trust and Acceptance:** The following should be taken into consideration regarding ethical issues for the users to trust the IDS and there should be provisions made for opt-in/opt-out where appropriate.
- **Ethical AI Usage**: The system should be developed without racial, gender or regional biases in security threat detection to guarantee fairness in the system's performance.
- **Responsible Disclosure**: Any vulnerabilities discovered during the development should be responsibly reported and fixed and not taken advantage of.

2. Requirements

2.1 Technical Requirements

- Utilize AI powered Intrusion Detection Systems (IDS) that leverage machine learning techniques to identify and address cybersecurity risks.
- Implement real time monitoring of network traffic to detect threats, like viruses and unauthorized entries.
- Create a detection system that blends signature based and anomaly-based methods to identify both unfamiliar security risks.
- Automatically act against threats such as blocking IPs sending out alerts. Isolating devices that have been compromised.
- •Enable the ability to detect communication standards, like MQTT, CoAP, HTTP, Zigbee and Bluetooth to support multi-platform monitoring.
- Incorporate with security systems, for IoT to establish layers of defense mechanisms.

3. Implementation Strategy

3.1 Machine Learning Model Development

- Utilize supervised learning models for detecting previously known threats.
- Deploy unsupervised learning techniques such as clustering and anomaly detection to identify novel attack patterns.
- Implement reinforcement learning for adaptive security measures based on network behavior.
- Use real-time extraction techniques to improve efficiency in large IoT networks.

4. Conclusion

This document describes the goals, needs, limitations and moral considerations for the Intrusion Detection System meant for IoT Devices. The aim of IDS is to deliver a security system that can scale, adapt and use AI technology to defend against cyber risks within IoT environments.

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/