

QUALIFYING PAPER

For the degree of

bachelor

topic: NETWORK INTRUSION DETECTION SYSTEM FOR IOT

Submitted by: fourth year student , group ICI-43
specialty 123 Computer Engineering

(code and name of specialty)



(signature)

Eneji Fredrick .O.

(surname and initials)

Supervisor

(signature)

Zharovskyi R.

(surname and initials)

Standards verified by

(signature)

Tysh Ie.

(surname and initials)

Head of Department

(signature)

Osukhivska H.

(surname and initials)

Reviewer

(signature)

Fryz M.

(surname and initials)

Ministry of Education and Science of Ukraine
Ternopil Ivan Puluj National Technical University

Faculty Faculty Of Computer Information Systems And Software Engineering
(full name of faculty)

Department Computer Systems And Networks Department
(full name of department)

APPROVED BY

Head of Department

Osukhivska H.M.

(signature)

(surname and initials)

29.12.2023

ASSIGNMENT
for QUALIFYING PAPER

for the degree of

bachelor

(degree name)

specialty

123 Computer Engineering

(code and name of the specialty)

student

Eneji Fredrick Oshana

(surname, name, patronymic)

1. Paper topic: Network Intrusion Detection System for IoT

Paper supervisor Zharovskyi Ruslan, PhD, Assoc.Prof.

(surname, name, patronymic, scientific degree, academic rank)

Approved by university order as 29 December 2024 №4/7-1247

2. Student's paper submission deadline 26.01.2024

3. Initial data for the paper IoT system structure, procols, machine learning algorithm

4. Paper contents: Introduction, 1. Analysis of subject area, 2. Project part, 3. Practical Part,
4. Occupation safety and health Conclusions

5. List of graphic material (with exact number of required drawings, slides)

1. OneM2M architecture

2. OneM2M IDPS strategy

3. Algoritms

4. Rezults graphics

6. Advisors of paper chapters

Chapter	Advisor's surname, initials and position	Signature, date	
		assignment was given by	assignment was received by
<i>Occupation safety and health</i>	<i>Lazaruk V.V. PhD, Assoc.Prof.</i>		

7. Date of receiving the assignment 29.12.2023

TIME SCHEDULE

LN	Paper stages	Paper stages deadlines	Notes
1	<i>Introduction</i>	<i>29.12.2023</i>	<i>Execute</i>
2	<i>Analysis Of Subject Area</i>	<i>05.01.2024</i>	<i>Execute</i>
3	<i>Analysis of Technical Task</i>	<i>11.01.2024</i>	<i>Execute</i>
4	<i>Project Part</i>	<i>15.01.2024</i>	<i>Execute</i>
5	<i>Practical Part</i>	<i>20.01.2024</i>	<i>Execute</i>
6	<i>Preparation to the qualification work presentation</i>	<i>22.01.2024</i>	<i>Execute</i>
7	<i>Qualification work presentation</i>	<i>26.01.2024</i>	<i>Execute</i>

Student

(signature)

Eneji Fredrick .O.

(surname and initials)

Paper supervisor

(signature)

Ruslan Zharovskyi

(surname and initials)

ABSTRACT

NETWORK INTRUSION DETECTION SYSTEM FOR IOT // Qualifying paper // Eneji Fredrick // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, group ICI-43 //Ternopil, 2024 // p. - 63, fig. – 12, bibl. - 17

Keywords: Internet of Things (IoT), Machine Learning, Intrusion Detection, Intrusion Prevention

With the expansion of the Internet of Things (IoT) and the evolution of attack techniques, IoT security has become a more critical concern. OneM2M is a global standardization initiative for the IoT, therefore its security implies the security of the IoT ecosystem. Hence, we focus our work on the security of the oneM2M standard.

In this thesis, we propose an Intrusion Detection and Prevention System (IDPS) based on Machine Learning (ML) for the oneM2M-based IoT systems. In order to adopt emerging technologies and especially with its interesting results already proven in the security domain, ML techniques are used in our IDPS strategy. Our oneM2M-IDPS detects potential threats and responds immediately. It detects and classifies threats on three different ML levels and reacts quickly with appropriate actions.

3MICT

INTRODUCTION.....	9
1 ANALYSIS OF SUBJECT AREA.....	11
1.1 Intrusion to IoT Threats and Security Mechanisms.....	11
1.2 Threat Landscape in IoT	12
1.3 Motivation and Problem Statement	15
2 PROJECT PART	20
2.1 OneM2M Standard and Security	20
2.1.1 OneM2M's Architecture Overview.....	21
2.1.2 OneM2M Security	23
2.2 OneM2M Threats.....	25
2.3 OneM2M-IDPS Challenges and Aims	26
2.4 OneM2M-IDPS Strategy	29
2.4.1 Data Acquisition and Features Extraction	31
2.4.2 Intrusion detection and prevention	31
3 PRACTICAL PART	37
3.1 Experimentation of Supervised Learning Algorithms for Intrusion Detection in OneM2M	37
3.1.1 Supervised ML Detections.....	38
3.1.2 The First Level of ML Detection.....	40
3.1.3 The Second Level of ML Detection.	42
3.1.4 The Third Level of ML Detection	43

					CS QP 123.008.00.00 EN			
<i>Ch.</i>	<i>Page</i>	<i>№ docum.</i>	<i>Sign</i>	<i>Date</i>				
<i>Develop</i>		<i>Eneji F.</i>			<i>Network Intrusion Detection System for IoT</i>	<i>Letter</i>	<i>Page</i>	<i>Pages</i>
<i>Supervisor</i>		<i>Zharovskyi R</i>					6	
<i>Reviewer</i>		<i>Fryz M.</i>				<i>TNTU, dept. CS, ICI-43</i>		
<i>N. Contr.</i>		<i>Tysh Ie.</i>						
<i>Approver.</i>		<i>Osukhivska H.</i>						

3.2	Effect of Dataset Size on Detection Results	44
4	OCCUPATIONAL SAFETY AND HEALTH	47
4.1	Medical aid in case of electric shock	47
4.2	Social importance of labor protection.....	50
	CONCLUSION	52
	REFERENCES.....	54
	Appendix A. Technical assignment	56

LIST OF ACRONYMS

IoT: Internet of Things

NIDS: Network Intrusion Detection System

M2M: Machine-To-Machine

IDS: Intrusion Detection System

TCP/IP: Transmission Control Protocol/Internet Protocol

API: Application Programming Interface

SSH: Secure Shell

DoS: Denial of Service

DDoS: Distributed Denial of Service

CVE: Common Vulnerabilities and Exposures

ML: Machine Learning

					<i>CS QP 123.008.00.00 EN</i>	<i>Page</i>
<i>Ch.</i>	<i>Page</i>	<i>Nº docum.</i>	<i>Sign</i>	<i>Date</i>		<i>8</i>

INTRODUCTION

The concept called the Internet of Things (IoT) stems back its roots since that very early 1980s where the very idea of connecting devices and enabling them to communicate had originated shaping up. The so-called father of ubiquitous computing Mark Weiser dreamed all about the objects and devices in future are embedded with a certain extent of smarts that facilitate seamless interactions to both the personal and the industry.

With the technological scenery, thus was sown a dream of a connected global network of devices. The IoT delivered the notable milestones of advancement achieved by IoT as it emerged from the invention of the RFID technology used to its wireless sensor network adaptation. At each stage, new opportunities and challenges emerged that redefined what laid ahead for IoT.

On the other hand, the evolution of utopia was happening side by side with these mushrooming security threats. However, in the beginning, there prevailed relatively moderate security issues based on mere basic encryption and authentication. But due to the highly increased rate of growth of IoT devices in this twenty-first century, it has been exponential thus this has presented a complex and dynamic security landscape.

This is based on a history from which IoT cybersecurity has developed to expose such threats from simple data breaches to well-coordinated attacks like the infamous Stuxnet worm. The history setting brings to the fore and highlights challenges in security resilience and drives home the message on the need for strong defence mechanisms especially within the network-based security.

With this background, the research seeks to answer the pivoting questions surrounding security to IoT networks. How has the growth in IoT transformed the security challenge? What are the challenges that Network Intrusion Detection Systems (NIDS) face as they adapt to the unique characteristics of environments created by IoT?

IoT security cannot be overemphasized. As IoT applications continue to expand into a critical component in infrastructure, healthcare, transportation, and smart cities, the significance of security breach fallout risks escalate by the day. The citadel of historical lessons suggests further pressing need to securing ourselves with improved defenses against cyber-threats in expanding the IoT environment.

					<i>CS QP 123.008.00.00 EN</i>	<i>Page</i>
<i>Ch.</i>	<i>Page</i>	<i>№ docum.</i>	<i>Sign</i>	<i>Date</i>		<i>10</i>

1 ANALYSIS OF SUBJECT AREA

1.1 Intrusion to IoT Threats and Security Mechanisms

Securing major concern for pervasive IoT systems demands an investigation on IoT threats the current defense mechanisms. Introducing the IoT security threat categories and its categorization has been done in this section while outlining the traditional defense techniques to give the reader a necessary security background towards comprehending this dissertation.

Security in the IoT arena differentiates from traditional systems and gives rise to unique challenges. Several factors attribute to this differentiation:

- IoT systems, including WSNs, are subject to constraints in terms of computational capability, memory capacity, battery life, and network bandwidth. Deploying resource-intensive traditional security solutions is impractical in such resource-constrained environments.

- Traditional centralized solutions will not work in guaranteeing protection for distributed and very heterogeneous IoT systems. The distributed aspect further introduces other complexities and constraints on their protection.

- IoT systems also operate within unpredictable physical environments, hence also introducing considerations of physical attacks as of concern alongside the rest of traditional security threats.

The connection of IoT systems to the internet exposes them to a new range of threats relating to the Internet as each device can now be accessed with its IP address.

- Constrained objects in the form of IoT devices generate a vast amount of data, hence leading to the eruption of an enormous sum of data. This increased the

					<i>CS QP 123.008.00.00 EN</i>			
<i>Ch.</i>	<i>Page</i>	<i>№ docum.</i>	<i>Sign</i>	<i>Date</i>				
<i>Develop</i>		<i>Eneji F.</i>			<i>ANALYSIS OF SUBJECT AREA</i>	<i>Letter</i>	<i>Page</i>	<i>Pages</i>
<i>Supervisor</i>		<i>Zharovskyi R</i>					11	
<i>Reviewer</i>		<i>Fryz M.</i>				<i>TNTU, dept. CS, ICI-43</i>		
<i>N. Contr.</i>		<i>Tysh Ie.</i>						
<i>Approver.</i>		<i>Osukhivska H.</i>						

risk of the device being subjected greatly to flooding attacks. There also is limited network bandwidth to prevent such attacks regularly.

- IoT systems incorporate protocols and technologies that are of a diverse nature into the same system. Any proposed solution for ensuring security in an IoT system thus has to factor in this diversity in protocols and technologies.

The following sections discuss two main topics on how IoT threats are classified as well as exploring conventional defense mechanisms.

1.2 Threat Landscape in IoT

Device Vulnerabilities: IoT devices are susceptible to various vulnerabilities such as default credentials, insecure firmware, and lack of regular security updates.

Data Interception: Man-in-the-middle attacks targeting communication between IoT devices can compromise sensitive data.

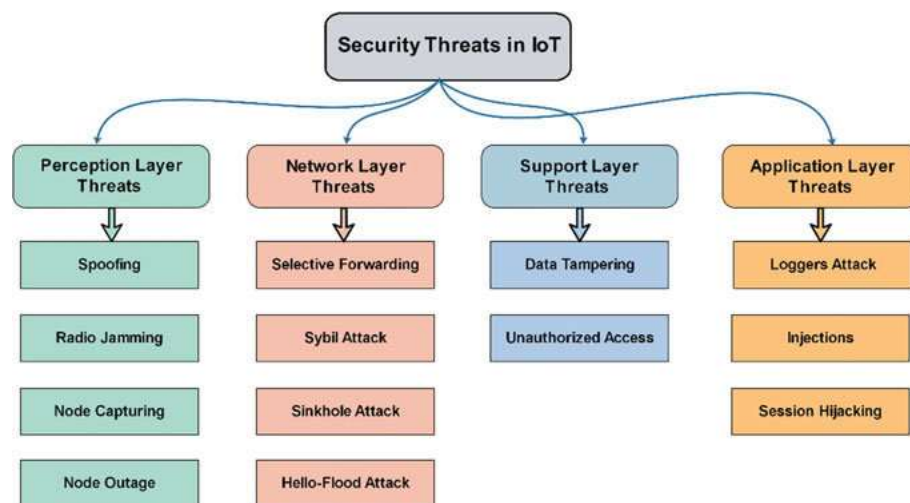


Figure 1.1 – Security threats at different layers of the IoT architecture

Network-Based Threats:

– Denial of Service (DoS): Malicious actors may attempt to overwhelm IoT networks with traffic, disrupting normal operations.

– Spoofing Attacks: Unauthorized devices may attempt to gain access by

impersonating legitimate IoT devices.

Unauthorized Access and Control:

- Authentication Weaknesses: Weak or compromised authentication mechanisms can lead to unauthorized access to IoT devices.
- Unauthorized Device Pairing: Attackers may attempt to pair unauthorized devices with the IoT network.

Data Security Concerns:

- Data Tampering: Manipulation of data transmitted between IoT devices can lead to false information and incorrect decision-making.
- Data Privacy Issues: Inadequate protection of user data collected by IoT devices poses privacy risks.

OSSEC-Based Security Mechanisms:

- Real-time Log Analysis: OSSEC excels in real-time log analysis, providing visibility into network activities and detecting anomalies.
- Custom Rule Development: OSSEC allows the creation of custom rules tailored to the specific communication patterns and behaviors of IoT devices.
- Active Response: OSSEC's active response capabilities enable immediate actions in response to security incidents, helping mitigate threats swiftly.

Device Profiling and Anomaly Detection:

- Device Profiling: OSSEC facilitates the creation of device profiles, allowing the system to understand and recognize normal behaviors for each IoT device.
- Behavioral Analysis: The NIDS, powered by OSSEC, employs behavioral analysis to detect anomalies and deviations from established device profiles.

Centralized Monitoring Console:

- Real-time Monitoring: The centralized monitoring console powered by OSSEC provides a centralized hub for real-time analysis of security events across the IoT infrastructure.
- Alert Prioritization: OSSEC helps prioritize alerts based on severity,

enabling a more focused response to critical security incidents.

Scalability and Performance Optimization:

- Scalability Planning: OSSEC's scalability features are leveraged to accommodate the diverse and growing nature of IoT deployments.
- Resource Optimization: OSSEC is optimized for performance, ensuring efficient intrusion detection while considering the resource constraints of IoT devices.

Incident Response Framework:

- Incident Identification: OSSEC assists in the rapid identification of security incidents through alerting and detailed logs.
- Automated Responses: OSSEC enables the automation of responses, allowing for immediate actions to mitigate the impact of security threats.

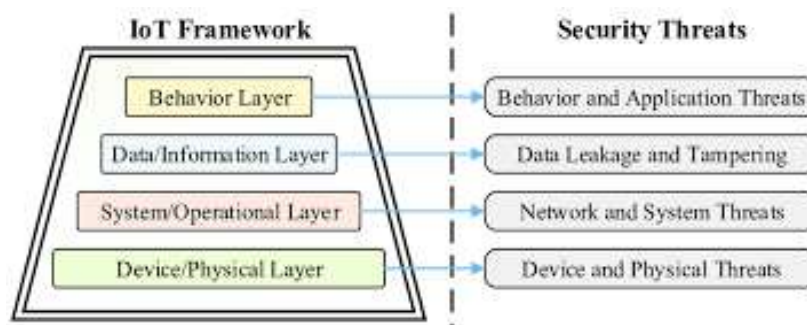


Figure 1.2 – Security threats model of IoT framework

Continuous Improvement and Adaptation:

Feedback Loop: OSSEC's feedback mechanisms contribute to continuous improvement by allowing organizations to learn from security incidents and refine intrusion detection rules.

Adaptation to Emerging Threats: OSSEC's flexibility supports adaptation to evolving IoT security threats through regular updates and rule enhancements.

IoT trouble orders:

1. Device- position pitfalls - Unauthorized Access Involves unauthorized access to IoT bias using dereliction credentials or weak authentication mechanisms.

-Physical Tampering pitfalls related to unauthorized physical access and tampering with IoT device factors.

2. Communication pitfalls - Wiretapping Unauthorized interception of communication between IoT bias. - Data Interception Targeting the interception of data transmitted between IoT bias.

3. Network- Level Threats - Denial of Service(DoS) Attacks aiming to disrupt normal IoT network operations. - Network Spoofing Involves the impersonation of licit bias on the network.

4. Data Security and sequestration pitfalls - Data Tampering Unauthorized revision of data transmitted or stored by IoT bias. - sequestration Violations Threats to the sequestration of stoner data collected by IoT bias.

5. functional pitfalls - Firmware Manipulation Unauthorized revision of IoT device firmware.

1.3 Motivation and Problem Statement

The widespread adoption of Internet of Things (IoT) technologies has ushered in a new era of connectivity and innovation, transforming the way we interact with our surroundings. From smart homes and industrial automation to healthcare and transportation, IoT devices have become integral components of modern ecosystems. However, this proliferation of interconnected devices has also given rise to unprecedented security challenges, necessitating advanced and adaptive defense mechanisms.

The motivation behind this project stems from the imperative to secure IoT environments against evolving cyber threats. Traditional security measures often fall short in addressing the unique characteristics and vulnerabilities inherent in IoT deployments. A dedicated and robust solution is required to ensure the confidentiality, integrity, and availability of data exchanged between IoT devices and to safeguard against potential malicious activities. In response to this critical

need, the implementation of a Network Intrusion Detection System (NIDS) specifically tailored for IoT, leveraging the capabilities of OSSEC, emerges as a strategic and proactive approach to fortifying IoT security.

The IoT landscape is characterized by diverse communication protocols, resource-constrained devices, and a multitude of device types, making it inherently susceptible to a wide range of security threats. Traditional defense mechanisms struggle to keep pace with the dynamic nature of these threats, leaving IoT ecosystems vulnerable to unauthorized access, data tampering, and other malicious activities.

The problem at hand is the lack of a dedicated and adaptive security infrastructure tailored to the intricacies of IoT environments within our organization. Current security measures do not provide the level of visibility and responsiveness required to effectively detect and mitigate potential security incidents in real-time. This gap exposes our IoT infrastructure to the following challenges:

- Inadequate Threat Visibility. Current monitoring tools lack the specificity to discern IoT-specific threats, leading to a lack of visibility into potential security incidents and anomalies.
- Resource Constraints of IoT Devices. Traditional intrusion detection systems may impose undue resource burdens on IoT devices, affecting their performance and compromising operational efficiency.
- Delayed Incident Response. The absence of a dedicated NIDS tailored for IoT results in delayed detection and response to security incidents, increasing the risk of data breaches and system compromise.
- Insufficient User Awareness. Inadequate user awareness and training on IoT security best practices contribute to an environment where potential threats may go unnoticed or unreported.
- Scalability Challenges. The organization's growing IoT deployment poses challenges in terms of scalability for existing security measures, necessitating a solution that can adapt and scale with the expanding IoT ecosystem.

– Contextualizing IoT Security Challenges. This subject area delves into the evolving landscape of the Internet of Things (IoT) and the consequential rise in security challenges. The increasing integration of diverse IoT devices into critical systems introduces unique vulnerabilities, necessitating a focused approach to security measures.

– Recognition of Specialized Security Needs. This analysis recognizes that the conventional security paradigms are ill-suited for the distinctive challenges posed by IoT environments. As IoT devices span various industries, employ different communication protocols, and exhibit resource constraints, a tailored security solution becomes imperative.

– Strategic Selection of OSSEC. This subject area strategically introduces OSSEC as a pivotal tool for addressing the security intricacies of IoT. The open-source nature, coupled with its proven efficacy in host-based intrusion detection, positions OSSEC as a flexible and adaptable solution to monitor and respond to security events in IoT networks.

– Initial Security Assessment. Emphasizing the importance of a comprehensive security assessment, the subject area outlines the initial steps required to understand the existing vulnerabilities and potential threat vectors within the organization's IoT infrastructure. This sets the foundation for a targeted and effective intrusion detection system.

– Customization for IoT Idiosyncrasies. Recognizing that off-the-shelf solutions may fall short, the analysis underscores the need to customize OSSEC to accommodate the nuances of IoT communications. Tailoring rules and configurations becomes crucial in aligning the intrusion detection system with the specific behaviors of diverse IoT devices.

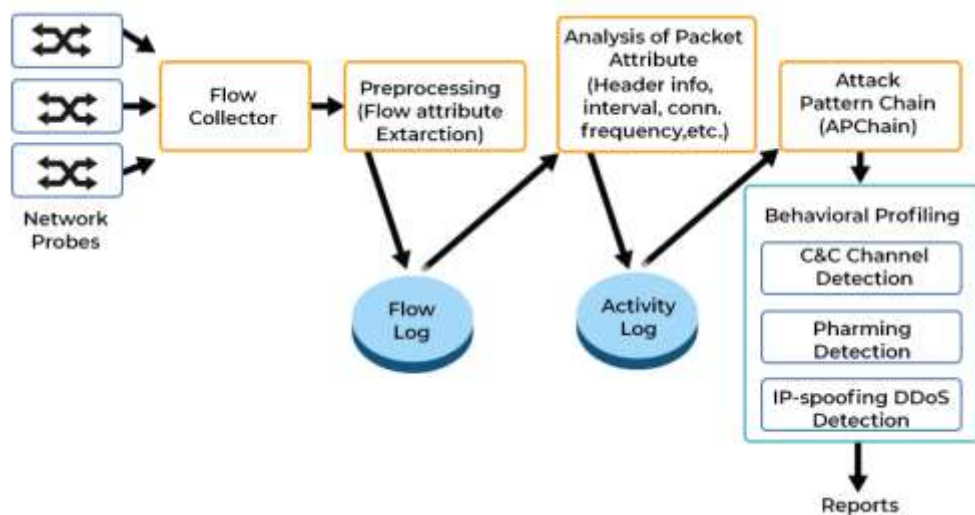


Figure 1.3 – Network Behaviour Analysis Using APChain Algorithm

- Device Profiling and Behavioral Analysis. The subject area highlights the significance of creating device profiles to establish a baseline for normal behaviour. By incorporating behavioural analysis, the intrusion detection system gains the capability to discern anomalies, thereby enhancing its accuracy in identifying potential security threats.

- Real-time Monitoring and Swift Response. The analysis emphasizes the importance of real-time monitoring through a centralized console for timely analysis of OSSEC alerts. The ability to respond swiftly to potential security incidents is paramount in minimizing the impact on IoT environments and ensuring operational continuity.

- Scalability Challenges and Resource Optimization. Addressing the scalability challenges in large-scale IoT deployments, the subject area acknowledges the need to optimize OSSEC for performance. This involves evaluating and enhancing the system to operate efficiently within the resource constraints inherent in many IoT devices.

- Development of Incident Response Framework. The subject area stresses the development of a comprehensive incident response framework based on OSSEC

alerts. Clearly defined procedures for isolating compromised devices and mitigating security incidents are crucial components in an effective cybersecurity strategy.

– Training and Knowledge Transfer. Recognizing the human element in cybersecurity, the subject area underlines the necessity of creating comprehensive documentation and conducting training sessions. Empowering the IT team with the knowledge required to manage and respond effectively ensures the sustainability of the implemented NIDS framework.

– Anticipated Outcomes and Significance. The analysis concludes by outlining the anticipated outcomes of the project, including a fortified IoT security infrastructure, reduced response time to incidents, heightened organizational awareness, and the establishment of a scalable NIDS framework. The significance of the project lies in its proactive approach to addressing current and future security risks in IoT deployments.

Conclusions to 1 chapter

The main contribution of this work is the design and the implementation of an IDPS based on ML to protect the Iot. To achieve this goal, we began by conducting a comprehensive review of the IoT security ecosystem.

It guides the reader in discovering the intersection of the three areas by providing all the necessary details to understand the security in IoT. The paper started by presenting and categorizing the IoT security threats as well as the traditional defense techniques with a focus on IDSs types.

2.1 OneM2M Standard and Security

In the world of Internet of Things (IoT), where heterogeneity dominates, thrives the OneM2M architecture as a unifying force, which presents a realized standardized framework to realize the seamless interoperability and communication amongst the various device types. With the present rate at which IoT ecosystems are springing up interconnected devices and platforms, an organized architecture is essential that can tap the capabilities of connected technologies.

Working as a connector, the sense the OneM2M architecture brings about is felt in how it breaks down barriers that do normally plague IoT spaces through its common language and set of protocols. Working as an integrator, amalgamating different connected devices and services taking place in various industries for them to communicate with one another and manage each other.

OneM2M architecture encapsulates a general, distinct layered framework that is regarded from infrastructure to application as embodied by a holistic approach of the deployment of IoT. It engenders relationships between hardware, networks, and applications in such a way data related activities and interactions can take place.

In this informative journey, we shall peel the layers of OneM2M architecture unravelling its components, enlighten it with its security mechanisms, and light it with its role in shaping the esteemed future of IoT ecosystems. This project report aims to explore and extract the role intricacies of OneM2M with its various characteristics and impact over today's developing landscape of connected technologies.

Such a framework as OneM2M architecture is a standardized model that has been designed with the aim to incorporate all the main features and layers

					<i>CS QP 123.008.00.00 EN</i>			
<i>Ch.</i>	<i>Page</i>	<i>№ docum.</i>	<i>Sign</i>	<i>Date</i>				
<i>Develop</i>		<i>Eneji F.</i>			<i>PROJECT PART</i>	<i>Letter</i>	<i>Page</i>	<i>Pages</i>
<i>Supervisor</i>		<i>Zharovskyi R</i>					20	
<i>Reviewer</i>		<i>Fryz M.</i>				<i>TNTU, dept. CS, ICI-43</i>		
<i>N. Contr.</i>		<i>Tysh Ie.</i>						
<i>Approver.</i>		<i>Osukhivska H.</i>						

represented in a common IoT domain, for the sake of interoperability and easy communication between various IoT things, platforms, and applications. The core structure of the architecture comprises several core components and layers meant to ensure easy data sharing and management being inside an IoT domain.

2.1.1 OneM2M's Architecture Overview

The OneM2M architecture assures scalability, flexibility, and interoperability of the whole oneM2M system given its horizontal and service-oriented approach within heterogonous IoT environments.

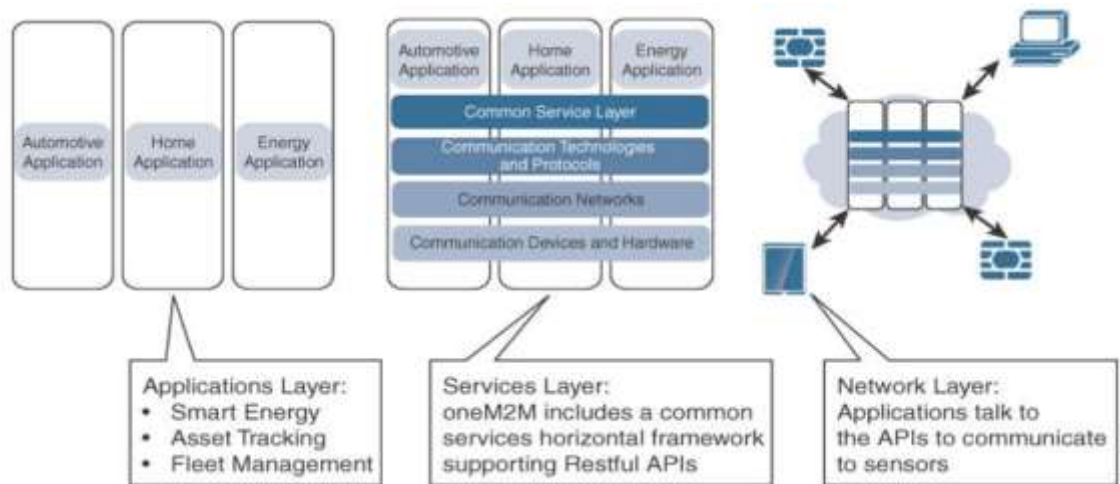


Figure 2.1 – The main element of the OneM2M architecture overview

Basically, it comprises among other things:

1) **Application Layer:** The representative of the interface, through which IoT applications interact with the underlying infrastructure, is at this layer. It usually hosts different components related to application enablement services and functionalities that include data management, device discovery as well as service provisioning.

2) **Common Services Layer:** This is the layer that groups together common functionalities as provisioned by different IoT applications deployed in diverse domain contexts. Security, access control, device management, data storage are some of the common services accomplished at this layer such that there is

standardization and consistency of operations across heterogeneous IoT environments.

3) Infrastructure Layer: In the infrastructure layer, the physical layers of IoT devices, sensors, actuators, and gateways are connected to the supporting underlying network infrastructure. At the infrastructure layer, data transmission tasks establish tasks for device communications and for network management tasks which provide a stable and efficient operating environment for running and managing IoT deployments.

4) Interworking Layer: The interworking layer provides and facilitates backward compatibility that provides migration paths towards architectures based on OneM2M, without disruption and enables seamless communication for the systems compatible with the previous devices of IoT with OneM2M. It also provides interoperability and integration to existing IoT protocols, standards, and communication technologies.

Key Features and Functionalities:

- Interworking: The OneM2M architecture potentially sets standards in interworking with the help of interfaces, protocols, and data models that facilitate successful interaction between various IoT devices and platforms.

-Scalability: The architecture model is natively scalable able to support millions of devices and applications in complex IoT deployments. Leveraging distributed computability principles and infrastructure elements that can scale to high threshold, the architecture can be used to achieve needs with broad growing requirements within the capacity of the accelerating demands in the environments needed for the realization of the power emanating from the IoT ecosystems.

- Flexibility: OneM2M is flexible and modular architecture that could be tailored as well as extended in accordance with specifications around specific use cases, requirements, and deployment scenarios. Organizations have freedom for tailoring it on their whims but only if it is part of standardized intra-interfaces and protocols involved in customization.

- Security: The security has carved out as an inbuilt part of the OneM2M architecture. It incorporates various kinds of authentication, authorization with the help of setting up encryption methods and enforced secured data transmission. Security has adapted industry states the art practices and carried out numerous best practices towards combating possible threats and vulnerabilities.

The OneM2M architecture offers building interoperable and scalable IoT solutions with consistent standard approach. It supports the unrestricted communication, incorporation, and supervision of the devices and applications in IoT without an obstruction throughout fields and industries with a comprehensive and horizontal service-oriented mobile architecture. In a digital era where most of the organizations have been embracing IoT technologies, this thereby makes the architecture upon which OneM2M lies an essential ground towards driving innovation, efficiency as well as connectivity.

2.1.2 OneM2M Security

The primary concern in the IoT ecosystems where big chunks of sensitive data travel and process through interlinked devices and networks is definitely security. The OneM2M architecture also duly considers this aforementioned immediate necessity of security

OneM2M Security covers a broad set of protocols, standards, best practices and follows the guidelines which have been structured to manage risks and for safeguarding IoT assets from possible access in an unauthorised means, data losses through breaches, or attacks by malicious groups. Basically, OneM2M Security focuses on offering confidentiality, integrity as well as availability on the IoT services and the data.

Key Components of OneM2M Security:

1. Authentication and Authorization: OneM2M consists of authentication and authorization to make an identification of a user or device or application being authenticated as an entity in order to access any IoT resources. Hence it extends its

services for the access control in permission management ensuring that only the valid instances are allowed to contact with sensitive information and functionalities.

2. Data Encryption: An encryption process is one of the most important aspects that assures a security of the data sent between the different IoT devices and platforms. OneM2M employs strong encryption algorithms to encrypt the data-in-transit and data-at-rest thus allowing a secure privacy-ensured information exchange with no possibility for the data being intercepted or tampering against.

3. Secure Communication Protocols: These include HTTPS, CoAPs, and MQTTs supported by OneM2M, allowing for secured communication link establishment between the IoT devices and the servers via encryption. The mechanisms used include various cryptographic means to secure the channels and interchange of data.

4. Role-Based Access Control: mechanisms of role-based access control (RBAC) are deployed in OneM2M to implement fine-grained access policies based on roles and privileges associated with users. After defining the roles, mapping the permissions, the designers of OneM2M secure that access is given to the resource only accessed by the user for carrying out its work, task delegated to it.

5. Threat Detection and Response: OneM2M has a threat detection and response mechanism incorporated into its system to identify, and then mitigate or prevent vulnerability to, security breaches as they occur. Anomaly detection algorithms and intrusion detection systems (IDS) shall monitor IoT network activity for suspicious activities and shall report alerts, or indeed automated responses, when anomalies are detected.

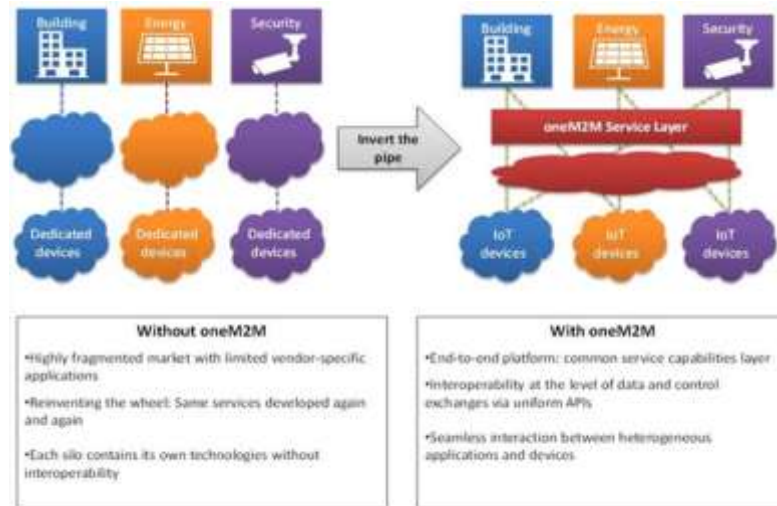


Figure 2.2 – Horizontal Platform OneM2M Security

In the exploration of OneM2M Security, we shall see more details on each of these components to look into their functionalities, implementations strategies as well as their effectiveness in securing the IoT executions from dynamic threats. We aim through this in-depth analysis to elucidate the vital role played by security layers in ensuring the trustworthiness and resilience of IoT ecosystems.

2.2 OneM2M Threats

This chapter explains some threats and vulnerabilities that might be there in any IoT based on OneM2M. For an IoT system, it is the case that risks can come from adversaries, but also from operational failures as well as weaknesses in software. Identification of such threats and its understanding is important for development of the proper security strategies and risks mitigations within IoT deployments.

First, we propose taxonomy for OneM2M threats which is designed to classify the diversity of types of threats that OneM2M systems may meet. Some of these types of threats include, but are not limited to unauthorized access, data breach, denial-of-service (DoS), spoofing, tampering, and insider threats.

We next consider the means by which attacks are carried forward against OneM2M-based IoT systems. This is based on real-world attack landscapes apart from how threats have been able to leverage from the existing vulnerabilities within the OneM2M architecture and protocols. By studying attack implementations, organizations thus bolster their threat intelligence as well as build proactive defence techniques that are intended to discourage potential risks.

In the following sections, we shall discuss briefly the importance of threat modelling and risk assessment in identification of specific, prioritized threats in OneM2M deployments. The process of threat modelling helps enterprises in analysis of threats systematically, visualization of probability to occur threat, visualizing impact of threat, and also in developing best countermeasures for effective risk mitigation.

We will also discuss how security best practice and standard is able to eliminate OneM2M threats. Following the existing security standards which include ISO/IEC 27001, NIST SP 800-53, OWASP IoT Top Ten will enable organizations to put in place a solid framework and guideline for OneM2M deployments.

In general, the awareness on the nature of threats and vulnerabilities that are part and parcel of any OneM2M-based IoT system will help organizations in devising and practicing the security countermeasures to protect their resources, take care of sensitive data, and to provide integrity, confidentiality, and availability to their IoT infrastructure.

2.3 OneM2M-IDPS Challenges and Aims

Marginal cases detected (covering challenges and aims of integration of Intrusion Detection and Prevention System (IDPS) with OneM2M)

Covering challenges and aims of integration of Intrusion Detection and Prevention System (IDPS) with OneM2M:

Challenges to Integration of IDPS with OneM2M:

1. Resource Constraints: These devices, in general, limit computational, memory, and energy resources. Traditional IDPS mechanisms cannot have direct application on IoT due to the limited computational power and memory, as well as demanding much processing power basing on the same.

2. Heterogeneity: With OneM2M, a wide variety of IoT devices and protocols coexist in its domain, therefore creating a heterogeneous environment. Such kind of heterogeneity makes it virtually impossible to invent uniform security standards and then apply that over the diverse set of devices and platforms, hence the integration process and the issues of making IDPS compatible become difficult.

3. Dynamism: Devices present in IoT environments are highly dynamic, keep joining and leaving the network at a high pace. Traditional IDPS solutions may not be effective enough to cope with such change dynamics hence creating management gaps from the security point of view.

4. Data Volume and Velocity: At high velocities, the IoT systems produce massive amounts of data. The processing of this data and identification of these attacks in real-time is quite a challenging task if the IDPS solution does not have the highly scalable and efficient capabilities to observe the reality of modern security threats.

5. Issues related to privacy: This poses a major issue as many IoT devices retain loads of sensitive information related to users' interests. While at the same time being able to effectively detect and prevent security attacks, the users' privacy as well as data need to be protected and assured from the IDPS mechanisms perspective.

6. Interoperability: Interfacing the devices to comply with OneM2M and IDPS solutions available from diverse vendors is quite a challenge. The interfaces and protocols need to be standardized so that varied components of IoT can easily interact and communicate with each other.

Objective for Integration of IDPS with OneM2M:

1. Real-time Threat Detection: The most critical and compelling aim for the IDPS integration with OneM2M is to ensure that there are real-time detection and reaction to threats. Monitor, continuously, network traffic as well as device behavioral pattern variation such that be curtailed prior menace corresponding to any security breach arise.

2. Flexibility and Expansion: The IDPS solutions should be flexible enough to change with the greater nature of IoT landscapes and scalable enough to accommodate the increasing number of devices and amounts of data. Deployment and management flexibility would thus allow IDPS systems to grow or actualize with the shift in IoT ecosystems.

3. Intrusion Detection and Prevention: IDPS should put into use advanced techniques detecting anomalies in the activity behavior. IDPS solutions will be able to monitor and detect anomalous or suspicious activities and alert IT personnel about potential security problems through the development of standard profiles about IoE devices and networks.

4. Standardization and Compatibility: Assurance of IDPS solutions compliance while keeping them compatible with integration and interoperability facilitation in the OneM2M standard. Compliance with the industry security standards keeps conformity and compatibility with various IoT deployments thereby mitigating challenges associated with the use of standardized security measures.

5. Efficient Resource Utilization: The IDPS solutions are to be resource efficient enough to lower the computational overhead related to IoT devices, though being effective from a security point of view. Hence, optimization techniques such as lightweight algorithms and distributed processing become enablers for security effectiveness.

6. Privacy Preserving: The privacy of sensitive data collected by IoT devices can be safeguarded via privacy-preserving techniques in IDPS mechanisms. This reduction in the collection will not occur when there is utilization of encryptions, anonymization, and access control mechanisms that will ensure the user's privacy

does not violate and unauthorized access to those pieces of information must not be carried out.

7. Collaborative defence mechanisms: Enabling collaboration of IDPS solutions deployed across multiple domains of IoT improves collective defence against emerging threats. Collaborative analysis and sharing with information facilitate accelerated incident responses, thereby overall increasing security of the IoT.

The above goals and challenges require to be addressed holistically by blending expertise from cybersecurity, network protocols, data analytics, and IoT architecture. Continual research and innovation are the most essential aspect which can lead to responsive and robust IDPS solutions that can safeguard the IoT ecosystems from exponentially mutating security threats.

2.4 OneM2M-IDPS Strategy

This comprehensive section delineates the strategic blueprint for deploying the Intrusion Detection and Prevention System (IDPS) within the OneM2M architecture. It encapsulates a multifaceted approach encompassing diverse components and processes geared towards fortifying the OneM2M service layer against intrusions and security breaches.

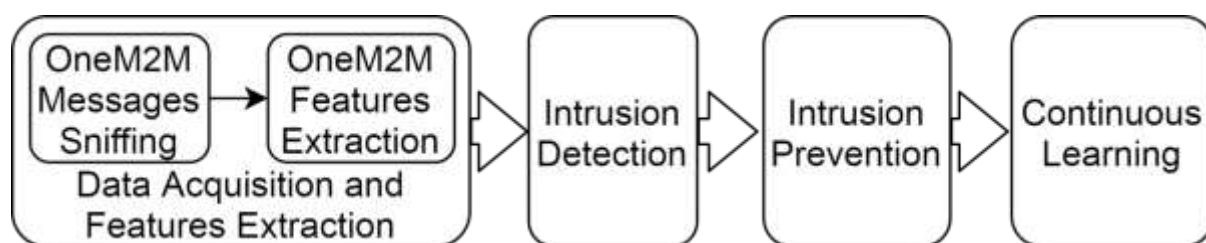


Figure 2.3 – OneM2M IDPS strategy

The strategy revolves around several key pillars:

1. Comprehensive Assessment of OneM2M Environment:

- The initial phase involves conducting a thorough assessment of the OneM2M environment, encompassing network topology, device configurations, data flows, and communication protocols. This holistic understanding serves as the foundation for designing tailored security measures.

2. Identification of Vulnerabilities and Threats:

- Employing robust vulnerability assessment tools and methodologies to identify potential weaknesses and threats within the OneM2M ecosystem. This proactive approach enables preemptive mitigation of vulnerabilities before they can be exploited by malicious actors.

3. Selection of Appropriate Security Mechanisms:

- Based on the assessment findings, selecting and implementing appropriate security mechanisms and protocols to safeguard the OneM2M service layer. This includes encryption, authentication, access control, and secure communication protocols tailored to the unique requirements of the OneM2M framework.

4. Integration of Intrusion Detection and Prevention Capabilities:

- Integration of sophisticated intrusion detection and prevention capabilities seamlessly into the OneM2M architecture. This involves deploying intrusion detection sensors strategically across the network to monitor and analyze network traffic in real-time, coupled with proactive prevention measures to thwart potential threats.

5. Continuous Monitoring and Analysis:

- Establishing a robust framework for continuous monitoring and analysis of network activities and security events within the OneM2M environment. This includes real-time alerting, log analysis, and correlation of security events to detect and respond to anomalies and potential security breaches promptly.

6. Response and Remediation Strategies:

- Developing well-defined response and remediation strategies to address detected security incidents effectively. This includes incident response protocols,

containment measures, and restoration procedures to minimize the impact of security breaches and ensure business continuity.

7. Ongoing Optimization and Adaptation:

- Continuously optimizing and adapting the IDPS strategy based on evolving threat landscapes, emerging vulnerabilities, and changing regulatory requirements. This entails regular security audits, threat intelligence analysis, and updates to security policies and configurations.

By adhering to these strategic imperatives, organizations can enhance the resilience of the OneM2M service layer against intrusions and security threats, fostering a secure and trusted IoT ecosystem. The IDPS strategy serves as a proactive defense mechanism, safeguarding critical assets, preserving data integrity, and instilling confidence among stakeholders in the reliability and security of OneM2M deployments.

2.4.1 Data Acquisition and Features Extraction

This module captures the oneM2M dispatches to be anatomized, reused and amended. It sniffs the oneM2M flows composed of a brace of Request and Response. also, features are uprooted and reused to construct the GFlows that are fed to the intrusion discovery module

2.4.2 Intrusion detection and prevention

This section meticulously outlines the workflow for managing detected intrusions within the OneM2M environment. It delineates a structured approach encompassing analysis, response, and mitigation steps to address security incidents effectively.

The data acquisition and the features extraction phase has generated a list of GFlows which is the input to the IDS module. In order to have an efficient detection, we treat the GFlows in a "last in first out" (LIFO) order. All the GFlows will be analyzed in the end but with a notion of priority for the most recent exchanged

messages. The processing of all GFlows is important in order to have a complete trace of the devices status over time.

After each analysis of a GFlow, the state "NORMAL", "UNKNOWN THREAT" or the exact type of the threat, is sent to the cloud in a Json format. The message contains the device identifier, the message identifier, the GFlow timestamp, the state as well as a description if needed.

The Prevention Workflow includes the following key stages:

1. Detection and Analysis:

- Upon detection of suspicious activities or anomalies within the OneM2M network, the IDPS initiates a comprehensive analysis to ascertain the nature and scope of the intrusion. This involves examining network logs, traffic patterns, and anomaly detection alerts to identify potential security breaches.

2. Incident Classification:

- The detected intrusions are classified based on severity, impact, and potential risk to the OneM2M ecosystem. Incidents are categorized into different threat levels to prioritize response and mitigation efforts accordingly.

3. Response Planning:

- A well-defined response plan is formulated to address each identified security incident effectively. This includes defining roles and responsibilities, establishing communication channels, and coordinating response actions across relevant stakeholders.

4. Containment and Mitigation:

- Immediate containment measures are implemented to prevent the spread of the intrusion and minimize its impact on the OneM2M infrastructure. This may involve isolating affected devices, blocking malicious traffic, and applying access controls to limit unauthorized access.

5. Forensic Analysis:

- Post-incident forensic analysis is conducted to gather evidence, identify the root cause of the intrusion, and assess the extent of the damage. Forensic data

analysis aids in understanding the attack vectors, refining detection mechanisms, and strengthening preventive measures for future incidents.

6. Remediation and Recovery:

- Once the intrusion is contained, efforts are directed towards restoring the integrity and functionality of the OneM2M environment. This involves patching vulnerabilities, restoring compromised systems, and implementing additional security controls to prevent recurrence of similar incidents.

7. Documentation and Reporting:

- Thorough documentation of the incident response process is maintained, including detailed logs, incident reports, and post-mortem analyses. Reporting mechanisms ensure transparency and accountability, facilitating regulatory compliance and stakeholder communication.

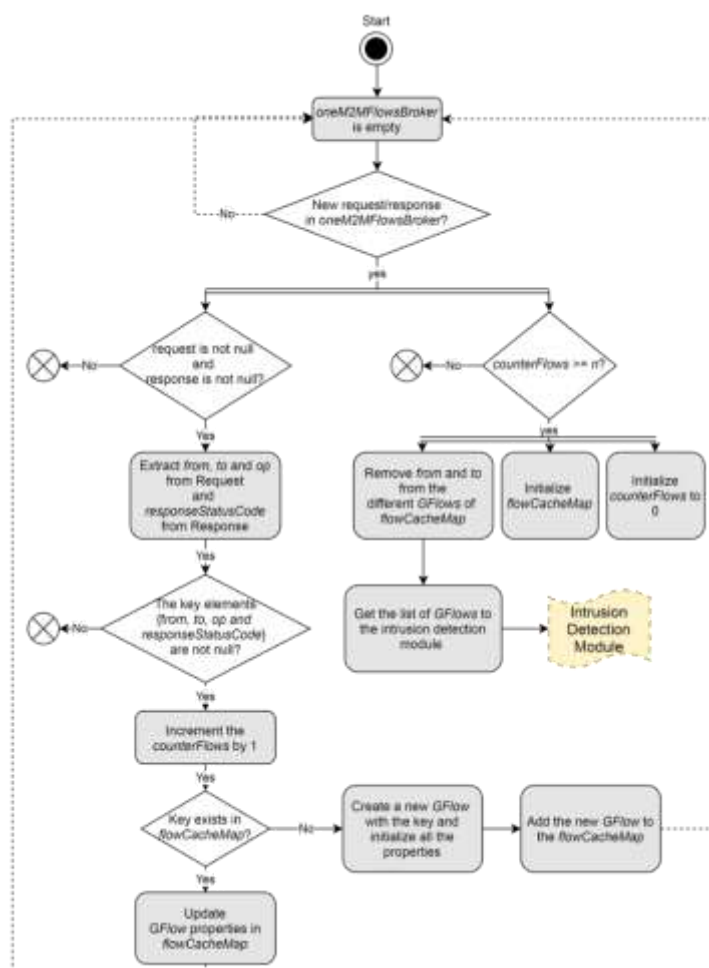


Figure 2.4 - Workflow of the oneM2M features extraction module

Ch.	Page.	Nº docum.	Sign	Date

authentication, role-based access controls, and encryption of data in transit and at rest.

4. Network Segmentation and Isolation:

- Implementation of network segmentation and isolation strategies to compartmentalize the OneM2M infrastructure and limit the lateral movement of attackers in the event of a security breach. Network segmentation helps contain the impact of intrusions and prevent the spread of malware and malicious activities.

5. Proactive Patch Management:

- Timely application of security patches and updates to mitigate known vulnerabilities and software flaws within the OneM2M ecosystem. Proactive patch management reduces the attack surface and minimizes the likelihood of successful exploitation by threat actors.

Continuous Learning:

This final section underscores the imperative of continuous learning within the IDPS framework to adaptively respond to evolving threats and emerging attack vectors in the OneM2M ecosystem. It emphasizes the importance of proactive monitoring, feedback mechanisms, and iterative refinement of intrusion detection and prevention strategies to maintain the efficacy and relevance of the IDPS framework over time.

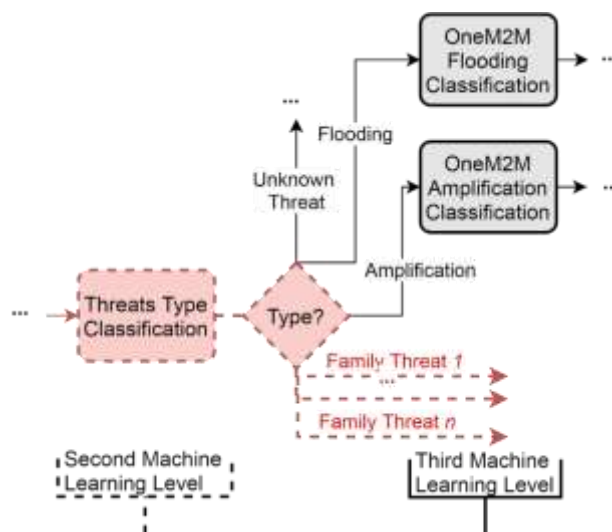


Figure 2.6 - Continuous Learning of families of threats

Key aspects of Continuous Learning include:

1. Threat Intelligence Integration:

- Integration of threat intelligence feeds and security research findings to stay abreast of the latest threat landscape and emerging attack trends relevant to the OneM2M environment. Threat intelligence enables proactive threat hunting, threat modeling, and risk assessment to identify potential vulnerabilities and preemptively mitigate security risks.

2. Anomaly Detection and Behavioral Analysis:

- Leveraging advanced anomaly detection and behavioral analysis techniques to identify subtle deviations from normal patterns of behavior within the OneM2M network. Continuous monitoring and analysis of network traffic enable the timely detection and response to anomalous activities indicative of potential security breaches.

3. Adaptive Security Controls:

- Implementation of adaptive security controls that dynamically adjust security policies and configurations based on real-time threat intelligence and risk assessments. Adaptive security controls enable the IDPS framework to adaptively respond to evolving threats and emerging attack vectors, minimizing the window of exposure and reducing the likelihood of successful intrusions.

4. Post-Incident Analysis and Lessons Learned:

- Conducting comprehensive post-incident analysis and lessons learned exercises to identify areas for improvement, root cause analysis, and mitigation strategies. Post-mortem analyses help refine detection mechanisms, enhance incident response procedures, and strengthen preventive measures to mitigate the risk of future incidents.

In essence, the concept of Continuous Learning underscores the proactive and iterative nature of the IDPS framework, emphasizing the importance of adaptability, resilience, and agility in effectively combating evolving threats and safeguarding the integrity of the OneM2M ecosystem.

3 PRACTICAL PART

In this chapter on the detection module with its three Machine Learning (ML) levels. We experiment with different ML and DL algorithms for each detection level in order to choose the most appropriate and efficient ones. We start this chapter by explaining our choice to adopt ML and Deep Learning (DL) techniques for the detection levels. Then, we present the metrics we relied on to evaluate the effectiveness of each algorithm in our oneM2M intrusion detection context, as well as the experimental environment. Furthermore, we concentrate on each detection level experiments; we introduce the used ML and DL algorithms (definitions, tools and frameworks), display the results and compare them with each other to finally choose the most appropriate one for each detection level. In addition, we are conducting some experiments on the effect of training data size and balance on detection results. In the last section of this chapter, we examine the one-class classification approach for both the first and second ML detection levels. For the first level which is the most crucial one that will affect the overall oneM2M-IDPS performance, such an approach highlights the detection of any behaviour different from normal (known for anomaly detection). For the second level, the one-class classification approach will be used to enable the unknown threats detection (called novelty detection).

3.1 Experimentation of Supervised Learning Algorithms for Intrusion Detection in OneM2M

In this section, we examined different supervised ML algorithms for the three ML detection levels. We chose supervised ML because the experiments conducted

					CS QP 123.008.00.00 EN			
<i>Ch.</i>	<i>Page</i>	<i>№ docum.</i>	<i>Sign</i>	<i>Date</i>				
<i>Develop</i>		<i>Eneji F.</i>			Practical part	<i>Letter</i>	<i>Page</i>	<i>Pages</i>
<i>Supervisor</i>		<i>Zharovskyi R</i>					37	
<i>Reviewer</i>		<i>Fryz M.</i>				TNTU, dept. CS, ICI-43		
<i>N. Contr.</i>		<i>Tysh le.</i>						
<i>Approver.</i>		<i>Osukhivska H.</i>						

in this section fall within the context of classification where we know already the classes into which the model should categorize the GFlow. This section will be divided into two main parts. The first section will treat supervised ML detections for the three levels. In the second one, we study the effect of size and balance of training dataset on the detection process

3.1.1 Supervised ML Detections

We begin this part with the definition of the experienced ML algorithms as well as the used tools. Then, for each detection level, we display the results, compare them and choose the most appropriate for each one.

Native Bayes (NB) is a probabilistic classifier based on Bayes' theorem. classifier can handle continuous and categorical data.

Support Vector Machine (SVM) is a classifier based on finding the best hyperplane (in the feature space) separating two data classes by maximizing the distance between the hyperplane and the closest data points of each class.

Decision Tree (DT) is a tree-like structure composed of decision nodes, branches and leaf nodes. A decision node represents feature (or attribute), the branch represents the conjunction of features that lead to the leaf nodes which represent the classification classes. DT can work with discrete as well as continuous value attributes. It learns to partition on the basis of the attribute value.

Random Forest (RF) is one of the popular ensemble classifiers that combines many DT. Each tree picks randomly a data features as input, processes DT algorithm, then by majority or weighted voting, the forest generates the prediction result.

Deep Neural Networks (DNN) is an application of artificial neural networks (ANNs) with multiple hidden layers. It consists of at least three layers.

For the four first ML algorithms, we use Weka 3 tool (developed in Java) which offers a collection of ML algorithms for data mining tasks in an easy-to-use software. It supports different modes of use: command line, GUI, Java API, and so on. We first use the GUI mode to facilitate the testing of the algorithms, then once the best algorithm is chosen, we integrate it into our IDPS using the Java API since

the used oneM2M implementation (Codex Data Platform IoT) is developed in Java. Implementations of the NB and RF classifiers in Weka are named after the original algorithms. However, for DT, we work with J48 which is an open source Java implementation to generate a pruned or unpruned DT. For SVM, we adopt SMO which is the implementation of John Platt's Sequential Minimum Optimization algorithm for the SVM classifier.

Regarding the parameters of the algorithms, we tried different configurations, either for the first, or for the last detection level. In the end, as there are no big changes in results, we chose the default parameters as proposed by Weka.

For the DL, we used the Python Deep Learning library Keras [Ker19b]. In order to obtain good detection results with DNN, different hyper-parameters have to be adjusted until the best combination is found. There are two types of hyper-parameters:

1. Hyper-parameters for the layers:

- the number of hidden layers reflects the number of layers deployed outside the input and output layers,
- the number of units in each layer which is an integer hyper-parameter that represents the dimensionality of the output space,
- the activation function for each layer is an important feature in the artificial neural networks. It decides the relevance of the neuron information with a non linear transformation.

- the kernel initializer for each layer defines the way to set its initial weights

2. Hyper-parameters for the learning process:

- the loss function which represents the objective function that the model will try to minimize by changing the parameters (weights) of the model,
- the optimizer in machine learning is a function that describes how to adjust the parameters of the model for the loss minimization.

Scikit-learn library, a general ML library built on top of NumPy¹, was also used for pre-processing operations such as the standardization and scaling of data.

3.1.2 The First Level of ML Detection

Our first experiments in the search for the best algorithm have been applied to our oneM2M dataset. We divide it into two files: the training dataset which is composed of 66% randomly chosen inputs and the test dataset which contains the 34% remaining values. The GFlows in both files are labeled as normal or threat. As discussed earlier, the parameters of shallow algorithms were the default ones proposed by Weka. However, for DNN we explored different combinations and the best results were achieved by a network of three fully connected layers. The input layer was initialized by normally distributed weights (random_normal initializer) and has a Rectified Linear Unit (ReLU) activation function. The second layer is composed of eight units with a random_normal as a kernel initializer and the sigmoid function for the activation. Regarding the output layer, it is a two units layer since we are in the context of binary classification. Softmax was the used activation function to guarantee a probability between 0 and 1 for each classification. The used loss function was the binary_crossentropy and the optimizer was the Stochastic Gradient Descent (SGD) optimizer.

Table 3.1 - Comparison of the results of the binary classification before the removal of duplicates

<u>ML algorithm</u>	<u>Recall</u>	<u>Accuracy</u>	<u>Precision</u>	<u>False Positive</u>	<u>Model Size</u>	<u>CPU Training</u>
	(%)	(%)	(%)	Rate (%)	(Ko)	Time (ms)
NB	79.70	71.05	80.90	53.70	10	800
SMO	98.60	84.14	83.20	57.10	15	36 968 840
J48	93.40	87.81	88.90	34.00	301	27 490
RF	89.90	83.84	88.50	33.50	307 673	138 010
DNN	97.41	86.91	86.61	13.39	18	596 463

As we can notice in Table 3.1, SMO achieves the best attack detection rate (recall) of 98.60%, followed by DNN and J48 with 97.41% and 93.40% respectively. However, SMO has the worst CPU training time. NB has the fastest learning phase and the smallest model compared to the rest. It reaches 800ms with 10Ko.

Unfortunately, NB has the poorest accuracy. It is J48 which has the best results in terms of accuracy and precision, with 87.81% and 88.90%. It is true that it has a larger model than the NB but 301Ko is still acceptable for IoT fog nodes. In addition, J48 is the second fastest algorithm to train. Regarding FPR, it is DNN which achieves the lowest rate with 13.39%, followed by RF (33.50%) and J48 (34.00%). Therefore, considering the overall metrics, we can say that J48, RF and DNN are the most efficient ones. But since RF model is heavy (138 010Ko), J48 and DNN remain the most appropriate algorithms for our binary classification task of the first level of ML detection.

After these results which were published in, we thought to re-move the duplicate entries from the oneM2M dataset which represent 4.27% of the initial data. The new results are compared in Table 3.2. As always, we use the default parameters for NB, SMO, J48 and RF. For DNN, we find that the best results were achieved by a network of three layers, as for the first case, however, the hidden layer is composed of 24 neurons with a ReLu activation function and we use categorical_crossentropy as a loss function and Adam as an optimizer. The network was trained for 200 epochs with a batch_size of 400.

As can be seen, the performance of NB, SMO, J48 and RF have improved proportionally compared to Table 3.1 (with a special enhancement for RF). However, DNN has poorer recall and FPR compared to its results with data containing redundant entries (especially for PFR: from 13.39% to 36.93%).

Table 3.2 - Comparison of the results of the binary classification after the removal of duplicates

ML algo- rithm	Recall (%)	Accuracy (%)	Precision (%)	False Positive Rate (%)	Model Size (Ko)	CPU Training Time (ms)
NB	82.40	73.63	82.30	52.40	10	620
SMO	98.70	83.10	84.10	53.3	15	10 854 250
J48	94.90	89.28	91.10	27.30	285	30 950
RF	92.50	87.78	91.30	26.20	172 360	172 618
DNN	93.10	87.01	88.40	36.93	21	162 000

Consequently, by process of elimination, we decide to use the J48 model for the first level of intrusion detection of our strategy.

3.1.3 The Second Level of ML Detection.

ML level detection identifies the threat family of an incoming GFlow if it is a known threat (flooding or amplification). If it is a new one that we have not seen before, the model needs to classify it as unknown. In this section, we will experiment only the classification of known family threats. The whole model with unknown threats detection will be discussed later in this chapter.

In this part, we use only the GFlows that are considered as threats in the oneM2M dataset with the labels corresponding to either flooding or amplification.

In Table 3.3, we compare the results of different ML algorithms for threat family classification experiments. J48 and RF achieve the best recall (100%), accuracy (99.98%) and precision (100%) with zero FPR. However, J48 is lighter and faster to train. DNN has close results (two fully connected layers with 2 neurons for the output layer, softmax as an activation function and categorical_crossentropy as a loss function). Regarding NB, it has the fastest CPU training time (1 080ms) and the smallest model (1Ko). Mean-while, it has the worst results in terms of the remaining metrics.

Table 3.3: Comparison of the results of the classification of threat families

ML algo-rithm	Recall (%)	Accuracy (%)	Precision (%)	False Positive Rate (%)	Model Size (Ko)	CPU Training Time (ms)
NB	93.30	93.30	93.60	3.30	11	1 080
SMO	99.90	99.88	99.90	0.20	15	556 710
J48	100	99.97	100	0	22	11 230
RF	100	99.98	100	0	1 761	113 850
DNN	99.87	99.90	99.97	0.05	16	15 696

3.1.4 The Third Level of ML Detection

The third ML level tends to identify the exact sub-type of a threat. At this point, we have flooding and amplification threats in the oneM2M dataset (Figure 3.12). As presented below, we experienced four shallow ML algorithms with Weka tool and DNN with Keras.

Flooding Classification For this experiment, we use only the flooding GFlows with the sub-types labels. As reported by Table 3.4, the J48 algorithm achieves the best results with 93.80%, 92.32%, 92.95% and 1.53% of detection rate, accuracy, precision and FPR, respectively. Even though, the NB algorithm is the one which generates the smaller model, 290 Ko (the size of the J48 model) is still always acceptable for the IoT context. Hence, we decide to adopt the J48 algorithm for the flooding classification.

Table 3.4 - Comparison of flooding-classification results

ML algorithm	Recall (%)	Accuracy (%)	Precision (%)	False Positive Rate (%)	Model Size (Ko)	CPU Training Time (ms)
NB	73.90	73.87	40	5	24	530
SMO	80.90	80.93	88.10	3.10	26	1 568 690
J48	93.80	92.32	92.95	1.53	290	9 280
RF	89.90	89.88	89.90	2.4	196 773	66 230
DNN	86.62	82.60	83.82	3.52	32	152 435

DT algorithms use the entropy computation technique for the features reduction. Tree based models calculate feature importance to keep the best performing features as close to the root of the tree. By analyzing the generated tree of J48 algorithm for flooding types classification, we remark that it eliminates 6 features from the oneM2M dataset features (Table 3.2): isSameFromTo, isToRemote, fromResourceType, counterSameFromOperationResponseType, counter SameTo ResponseType and counter-SameOperationResponseCategory. To inject a lighter

model into the fog nodes, we trained the flooding models with only the relevant features.

Amplification Classification Regarding the amplification classification (Table 3.5), the J48 algorithm achieves only the best accuracy (63.04%).

Table 3.5 - Comparison of amplification-classification results

ML algo rithm	Recall	Accuracy	Precision	False Positive Rate	Model Size	CPU Training Time
	(%)	(%)	(%)	(%)	(Ko)	(ms)
NB	49.00	49.03	46.70	27.70	12	320
SMO	68.40	58.96	64.60	17.90	16	1 505 340
J48	62.77	63.04	62.83	17.07	953	12 500
RF	63.70	63.74	64.00	16.80	211 092	41 560
DNN	61.28	63.43	60.81	16.80	29	126 504

SMO seems to have better recall (68.40%) and the best precision (64.60%). It is true that it does not have the best accuracy (6% less than J48), nor the best FPR (1% more than RF and DNN), nor the smallest model (4ko more than NB) but it remains the best in terms of overall performances. The only problem with SMO is its long CPU training time (about 25 minutes). Consequently, we decide to deploy the SMO model for the amplification classification.

3.2 Effect of Dataset Size on Detection Results

In this section, we consider two different cases related to data size that can affect the continuous learning module presented in Section 4.2.4. As detailed, this module needs to update ML detection models. For a quick training as well as an efficient consideration of new upcoming GFlows (without waiting for a large data availability), we need to find the minimum data size necessary to generate a reliable model. Fast training with a small amount of data generates lightweight and easily updatable models which is important in the security domain and interesting in the context of IoT and fog computing. First, we study the evolution of the models

performances in binary classification (first ML level) while decreasing the dataset size.

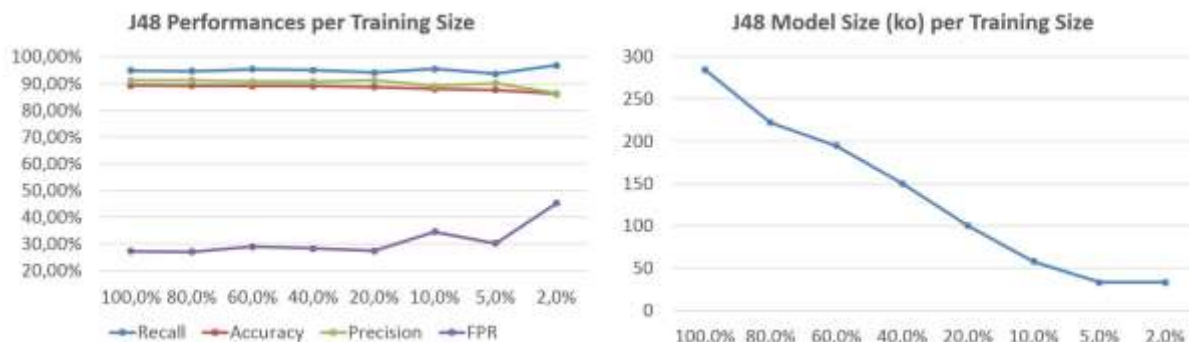


Figure 3.2 - Effect of training dataset size

The second experiment concerns the effect of data balance/imbalance on model performance (also for the first detection level). The testing dataset was extracted before the two experiments (34% of the whole dataset) and the percentages of data removed were chosen randomly. Both experiments were conducted on oneM2M dataset without redundant entries. In addition, we use the J48 algorithm since it had the best results in terms of threat detection for the first ML level

As presented in Figure 3.2 (left side), while decreasing the size of the training data, we note that the measures remain stable at the beginning until only 20% of the initial data remains. After 20%, the FPR starts to increase significantly. As expected, the size of the models decreases as the dataset decreases (Figure 3.2 right side). Consequently, for an acceptable ML performance, we can update the models with only 20% of the total oneM2M dataset size (only 44 654 GFlows instead of 223 273).

We continued our experimentation with the J48 algorithm. Since with only 20% of the initial data, J48 succeeded to have acceptable performances, we experimented our data balance on that basis.

We describe the imbalance of classes in terms of a ratio, i.e. 1 : 100 means that for every one example of normal GFlow, there are 100 examples of the other class which is threats.

First, in Figure 3.3, we fixed the amount of normal GFlows in the dataset and started to decrease the size of threat inputs. We found that the performance of the J48 remained acceptable up to the 100 : 160 ratio. After that, the recall and accuracy start to drop significantly.

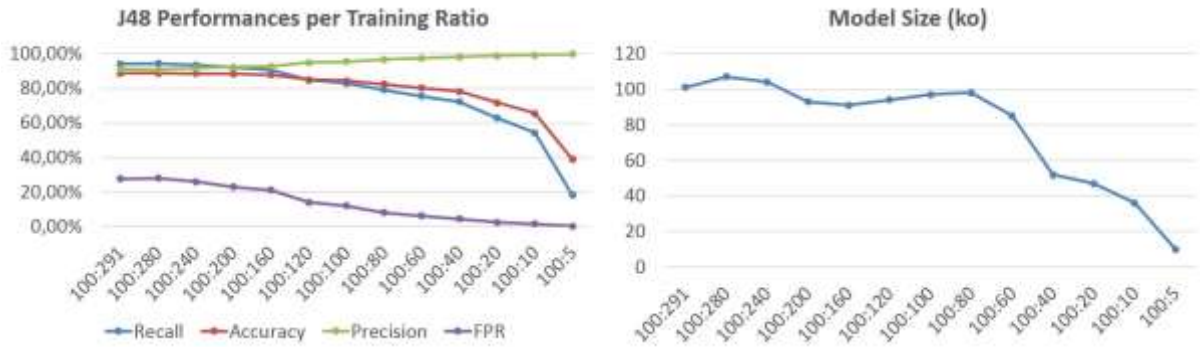


Figure 3.3 - Effect of data imbalance (decrease threat GFlows)

In Figure 3.4, we experimented the opposite.

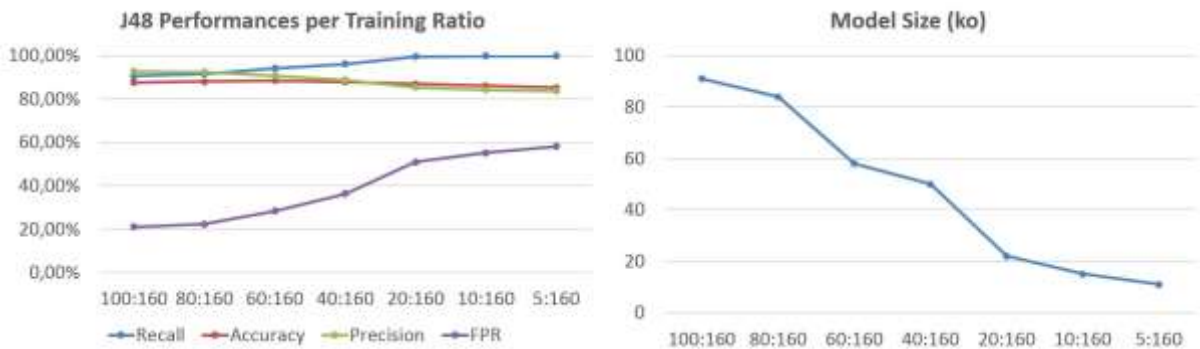


Figure 3.4 - Effect of data imbalance (decrease normal GFlows)

We started from the stable point of the last experiment which is a ratio of 100 : 160, we fixed the threat GFlows and started to decrease the number of normal inputs. We found that the most stable results are with ratios 100 : 160 and 80 : 160. Consequently, it is better to update the models starting from a ratio of 80 : 160.

4 OCCUPATIONAL SAFETY AND HEALTH

4.1 Medical aid in case of electric shock

Since the purpose of the work is related to the use of various electrical devices connected to the electrical network, we will consider the issue of actions in case of electric shock.

First of all, free the victim from the effects of the current, because from the duration of such action significantly depends on the severity of the electric injury. The safest way to free the victim from the effects of electric current is to turn off the electrical device that the victim touches, using the nearest switch, circuit breaker or other device for de-energizing.

The victim, after release from the electric current, can usually be in one of three states:

- If the victim is conscious, then it is necessary to put him on bedding of fabric or clothing, create an influx of fresh air, unbutton clothing that constricts and prevents breathing, rub and warm the body and ensure rest until the arrival of a doctor.
- The victim, who is in an unconscious state, should be given sniff ammonia or splash cold water on your face. When the victim regains consciousness, give him to drink 15-20 drops of valerian tincture and hot tea.
- In the absence of signs of life (breathing and pulse), it is necessary to immediately start cardiopulmonary resuscitation (CPR), because the probability of success is less the more time has passed since the onset of clinical death. CPR measures include artificial respiration and indirect heart massage.

Artificial respiration is performed by "mouth-to-mouth" or "mouth-to-nose" method. The person providing help exhales from his lungs into the lungs of the victim

					CS QP 123.008.00.00 EN			
<i>Ch.</i>	<i>Page</i>	<i>№ docum.</i>	<i>Sign</i>	<i>Date</i>				
<i>Develop</i>		<i>Eneji F.</i>			<i>Occupational safety and health</i>	<i>Letter</i>	<i>Page</i>	<i>Pages</i>
<i>Supervisor</i>		<i>Zharovskyi R.</i>					47	
<i>Consultant.</i>		<i>Lazaryuk V.</i>				<i>TNTU, dept. CS, ICI-43</i>		
<i>N. Contr.</i>		<i>Tysh Ie.</i>						
<i>Approver.</i>		<i>Osukhivska H.</i>						

directly into his mouth or nose, there is still enough oxygen in the air exhaled by the person

First, the victim must be placed with his back on a hard, flat surface, free from constricting clothing (unbutton the shirt collar, belt, loosen the tie), place a small roller of any material under the shoulder blades, tilt the head as far back as possible.

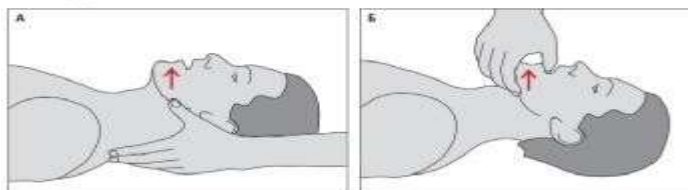


Figure 4.1 – Correct position of the victim's head

a - the rescuer turns the victim's head away with his left hand, at the same time supporting his neck with the right;

b - the rescuer holds the victim's head in a tilted position with the left hand, simultaneously pulling the lower jaw with the right hand.

Before starting artificial respiration, it is necessary to make sure patency of the upper respiratory tract, which can be closed by an inflated tongue, foreign objects, accumulated mucus.

The rescuer takes a deep breath, and then, tightly pressing his mouth through the gauze to the victim's mouth (at the same time, as a rule, covers the victim's nose with his cheek), blows air into the lungs, as shown in fig. 4.2. At the same time, the victim's chest expands. Due to the elasticity of the lungs and chest wall, the victim exhales passively. At this time, his mouth should be open. The frequency of air blowing should be 12 times per minute. Similarly, artificial respiration is performed by the "mouth to nose" method; at the same time, air is blown through the nose, and the victim's mouth must be closed.



Figure 4.2 – Mouth-to-mouth artificial respiration

You should be careful when performing artificial respiration: when the first signs of weak shallow breathing appear in the victim, it is necessary to adjust the rhythm of artificial respiration to it.

There are special means for artificial respiration, which, first of all, allow to avoid direct contact between the mouth of the victim and the mouth of the rescuer. In order not to harm the victim, the rescuer must be able to use such means.

In case of cardiac arrest, which can be determined by the absence of a pulse on the carotid artery and dilation of the pupils or in the case of heart fibrillation, it is necessary to carry out indirect heart massage simultaneously with artificial respiration. The victim is placed with his back on a hard surface, his chest is exposed, and the belt is unfastened. The rescuer stands to the left or right of the victim, placing his hands on the lower third of the chest (one on top of the other), energetically (with thrusts) presses on it. You need to press quite sharply, using the weight of your own body, and with such force that the chest bends 4-5 cm towards the spine. The required frequency is 60-65 clicks per minute.

Heart massage must be combined with artificial respiration. If CPR is performed by one person, measures to save the victim must be carried out in the following sequence: after two deep breaths into the mouth or nose, make 15 chest compressions, then repeat two breaths and 15 pressures to massage the heart. If two rescuers provide help, then one should perform artificial respiration, and the other should perform indirect heart massage, and during the air injection, the heart massage is stopped.

Measures for revitalization can be considered effective if the pupils have narrowed, the skin has started to turn pink (primarily, the skin of the upper lip), and

the pulse on the carotid artery can be clearly felt during massage strokes.

Thus, skillful provision of assistance in case of electric shockcurrent can save a person's life.

4.2 Social importance of labor protection

The social significance of labor protection lies in promoting the growth of the efficiency of social production through continuous improvement and improvement of working conditions, increasing their safety, reducing industrial injuries and occupational diseases.

The social importance of labor protection is manifested in growth labor productivity, preservation of labor resources and increase of the aggregate national product.

Labor protection consists in promoting the growth of production efficiency, which is achieved through continuous improvement and improvement of working conditions, increasing their safety, reducing industrial injuries and occupational diseases.

The increase in labor productivity occurs as a result of increasing the working time fund due to the reduction of intra-shift downtime by eliminating microtraumas or reducing their number, as well as due to the prevention premature fatigue through the rationalization and improvement of working conditions.

An important issue is the increase in labor productivity, which occurs as a result of increasing the working time fund due to the reduction of intra-shift downtime by eliminating microinjuries or reducing their number, as well as by preventing premature fatigue by rationalizing and improving working. Conditions and introducing optimal work modes and rest and other activities that contribute to increasing the efficiency of the use of working time.

The fact that the preservation of labor resources and the increase in the professional activity of working people occurs due to the improvement of the health condition and the extension of the average life expectancy through the improvement

of working conditions, which is accompanied by high labor activity and an increase in production experience. The professional level also increases thanks to the growth of qualifications and skills. Accordingly, the increase in the aggregate national product is due to the improvement of the above indicators and their constituent components.

Preservation of labor resources and increase in the professional activity of working people occurs due to the improvement of the state of health and the extension of the average life expectancy through the improvement of working conditions, which is accompanied by high labor activity and an increase in production experience. The professional level also increases thanks to the growth of qualifications and skills.

The increase of the total national product is due to the improvement of the above indicators and their constituent components. In addition, the social importance of labor protection is manifested in the growth of labor productivity, preservation of labor resources.

According to research, a set of measures to improve working conditions can increase labor productivity by 15-20%. Thus, the normalization of workplace lighting increases labor productivity by 6-13% and reduces shortages by 25%. Rational organization of the workplace increases labor productivity by 21%, rational painting of workplaces by 25%.

An increase in the effective working time fund can be achieved by reducing the temporary incapacity of workers due to illnesses and industrial injuries.

CONCLUSION

The proliferation of IoT devices globally has seen rapid growth in recent years, with deployments spanning various sectors such as healthcare, smart cities, and education. However, amidst this rapid commercialization, insufficient attention has been directed towards ensuring the safety and security of IoT networks and devices. This oversight poses risks to IoT users and threatens the broader Internet-connected ecosystem, including websites, applications, and servers. Moreover, security attack vectors have evolved in complexity and diversity, necessitating a deeper analysis of these threats, their detection, and strategies for infection prevention and system recovery post-attack.

In this thesis, we propose an Intrusion Detection and Prevention System (IDPS) leveraging Machine Learning (ML) techniques tailored for the IoT ecosystem. Our focus centers on the international oneM2M standard, facilitating communication among heterogeneous devices and applications through a common M2M Service Layer. Notably, our proposal represents the first IDPS designed specifically for the oneM2M service layer. It offers a comprehensive security framework encompassing data collection, threat detection, and the activation of appropriate responses. Furthermore, our IDPS features a continuous learning module, ensuring its adaptability to evolving threat landscapes.

The thesis is structured into 3 chapters. In general, provided above is an overview of the IoT security landscape, categorizing threats and discussing traditional defense mechanisms. Also outlined is the motivations and contributions of the research. We also review existing literature on network IDPS for IoT systems, including ML-based approaches, comparing strategies, architectures, and outcomes. We also introduced the oneM2M standard and its security mechanisms, highlighting threats to service availability and presenting a taxonomy and implementations for mitigating these risks.

					<i>CS QP 123.008.00.00 EN</i>	<i>Page</i>
<i>Ch.</i>	<i>Page.</i>	<i>№ docum.</i>	<i>Sign</i>	<i>Date</i>		52

We also delve into the challenges and objectives of our oneM2M-IDPS proposal, detailing its strategic framework and the architecture of its four modules: data acquisition and feature extraction, IDS, IPS, and continuous learning. Also we focus on the ML aspect of our IDPS, implementing detection modules with three ML levels using the oneM2M dataset. We experiment with various ML and Deep Learning algorithms, exploring supervised ML and one-class classification approaches for detection.

In summary, our research addresses critical gaps in IoT security, offering a comprehensive IDPS solution tailored to the unique requirements of the oneM2M standard. Through rigorous analysis and experimentation, we aim to enhance the security posture of IoT ecosystems and contribute to the resilience of Internet-connected infrastructure.

REFERENCES

1. S. Agrawal and J. Agrawal. Survey on Anomaly Detection using Data Mining Techniques. *Procedia Computer Science*, 60:708–713, January 2015.
2. S. A. Alabady, F. Al-Turjman, and S. Din. A Novel Security Model for Cooperative Virtual Networks in the IoT Era. *International Journal of Parallel Programming*, July 2018.
3. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys Tutorials*, 17(4):2347–2376, 2015.
4. M. E. Aminantoa and K. Kimb. Deep Learning in Intrusion Detection System : An Overview. In *International Research Conference on Engineering and Technology (2016 IRCET)*. Higher Education Forum, 2016., 2016.
5. F. Al-Turjman and S. Alturjman. Context-Sensitive Access in Industrial Internet of Things (IIoT) Healthcare Applications. *IEEE Transactions on Industrial Informatics*, 14(6):2736–2744, June 2018.
6. A. L. Buczak and E. Guven. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Communications Surveys Tutorials*, 18(2):1153–1176, 2016.
7. W. Ben Jaballah, M. Conti, G. Filè, M. Mosbah, and A. Zemmari. WhacA-Mole: Smart node positioning in clone attack in wireless sensor networks. *Computer Communications*, 119:66–82, April 2018.
8. H. Bostani and M. Sheikhan. Hybrid of anomaly-based and specificationbased IDS for Internet of Things using unsupervised OPF based on MapReduce approach. *Computer Communications*, 98(Supplement C):52–71, January 2017.
9. S. Babar, A. Stango, N. Prasad, J. Sen, and R. Prasad. Proposed embedded security framework for Internet of Things (IoT). In *2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information*

Theory and Aerospace Electronic Systems Technology (Wireless VITAE), pages 1–5, February 2011.

10. S. S. Basu, S. Tripathy, and A. R. Chowdhury. Design challenges and security issues in the Internet of Things. In 2015 IEEE Region 10 Symposium, pages 90–93, May 2015.

11. E. Benkhelifa, T. Welsh, and W. Hamouda. A Critical Review of Practices and Challenges in Intrusion Detection Systems for IoT: Towards Universal and Resilient Systems. IEEE Communications Surveys Tutorials, pages 1–1, June 2018.

12. Yatsyshyn V., Pastukh O., Palamar A., Zharovskyi R. Technology of relational database management systems performance evaluation during computer systems design. Scientific Journal of TNTU.Tern.: TNTU. 2023. Vol 109. No 1. P. 54–65.

13. Yatsyshyn V., Pastukh O., Zharovskyi R., Shabliy N. Software tool for productivity metrics measure of relational database management system. Mathematical Modeling. No 1 (48). 2023. P. 7-17.

14. N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki. Network Intrusion Detection for IoT Security based on Learning Techniques. IEEE Communications Surveys Tutorials, 2019.

15. Желібо Є. П. Заверуха Н.М., Зацарний В.В. Безпека життєдіяльності. Навчальний посібник. К.: Каравела, 2004. 328 с.

16. Зеркалов Д.В. Безпека життєдіяльності. Навчальний посібник. К.: Основа. 2011. 526 с.

17. Osukhivska H., Tiш Є.В., Паламар А.М. Методичні вказівки до виконання кваліфікаційних робіт здобувачів першого (бакалаврського) рівня вищої освіти спеціальності 123 «Комп'ютерна інженерія» усіх форм навчання. Тернопіль, ТНТУ. 2022. 28 с.

Appendix A.
Technical assignment

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
Ternopil Ivan Puluj National Technical University
Faculty of Computer Information Systems and Software Engineering

Computer Systems and Networks Department

“Approved”

Head of department

_____ Osukhivska H.M

“ ___ ” _____ 2024 p

NETWORK INTRUSION DETECTION SYSTEM FOR IOT

TECHNICAL ASSIGNMENT

Type of work:

Qualification work

Bachelor’s Degree

123 "Computer Engineering"

“AGREED”


Supervisor

_____ Zharovskyi R.

«____» _____ 2024 p.

“PERFORMER”

Student of Group ICI-43

 Eneji F.

«____» _____ 2024 p.

Ternopil 2024

1. Terms

The network intrusion detection system for IOT is a comprehensive security framework designed specifically for Internet of Things (IoT) environments. It employs state-of-the-art algorithms and sensors to continuously monitor network activities, detecting and thwarting unauthorized access, anomalies, and potential cyber threats within IoT ecosystems. By ensuring the integrity, confidentiality, and availability of transmitted and processed data, this system plays a vital role in safeguarding IoT devices and networks against malicious attacks, thereby enhancing overall system security and resilience.

The full name of the project is NETWORK INTRUSION DETECTION SYSTEM FOR IOT

1.1 Order For System Development

Performer Eneji Fredrick Oshana ICI-43, Computer engineering.

1.2 Input documents for System development

- Specification of Operating System supporting OneM2M model architecture
- Specification of Hardware for testing oneM2M architecture model
- Specification of OneM2M architecture model
- Documentation of OneM2M architecture
- Setting up the OneM2M model
- Integrating Datasets for OneM2M model.
- Testing IDPS cases before and after implementation of oneM2M model architecture

1.3 Date of Start And Submitting

- Planning date of start – 29.12.2023
- Submission date – 26.01.2024

1.4 The sequence of results presentation

Projects consist of the lists of documentation which responds to the approved requirements of the computer systems and networks department. Requirements response to the standards in the field of computer engineering development (ISO standards).

Presentation of intermediate results of the diploma project is carried out according to the schedule approved by the supervisor.

1.5 Standards and regulatory documents

1. ISO/IEC 27001:2013 - Information security management systems.
2. NIST SP 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations.
3. IEC 62443 - Industrial communication networks - Network and system security.
4. ENISA (European Union Agency for Cybersecurity) Guidelines for Securing the Internet of Things.
5. OWASP IoT Security Project - Provides guidelines and best practices for IoT security.

2 Appliance and Purpose Of System Design

The purpose of OneM2M is to establish a standardized framework for interoperable IoT systems, ensuring scalability, security, and innovation across diverse domains.

2.1 Appliance Of System

The OneM2M architecture model establishes a standardized framework for seamless communication among diverse IoT devices and platforms. Rooted in a layered structure, it consists of the Application Layer for user functionalities, the Common Services Entity (CSE) Layer for communication facilitation, and the Network Layer for infrastructure management. Emphasizing a resource-oriented

model, each entity is uniquely identified, promoting structured data and functionality management. This design addresses the challenge of IoT ecosystem heterogeneity, ensuring interoperability and scalability.

2.2 Objective Of The oneM2M

The OneM2M model in IDPS (Intrusion Detection and Prevention Systems) aims to strengthen IoT security by providing a standardized framework for effective communication and monitoring of diverse IoT devices. This integration establishes a unified environment, ensuring interoperability and seamless security measures across different IoT setups. With OneM2M's resource-oriented approach, IDPS can identify, manage, and monitor IoT entities, contributing to a robust and standardized security infrastructure. Ultimately, the goal is to fortify IoT systems against intrusions, ensuring reliability and integrity in the face of potential security threats..

2.3 Characteristic of Design Object

It consists of three main architectural layers:

1. Application Layer (AL): This layer represents the highest level and is where applications and services interact with the IoT system. It includes various applications, services, and functionalities specific to user requirements.
2. Common Services Entity (CSE) Layer: Positioned in the middle, the CSE layer serves as an abstraction layer, facilitating communication between the Application Layer and the Network Layer. It contains the following key components:
 - Application Entity (AE): Represents an application's functionality within the IoT system.
 - Container (CNT): Organizes resources and data within the AE.
 - Content Instance (CI): Contains the actual data or content within a resource.
3. Network Layer (NL): At the lowest level, the Network Layer deals with the communication infrastructure. It includes components such as:

- Interworking Proxy Entity (IPE): Ensures communication with non-OneM2M devices.
- Middle Node (MN): Facilitates communication within the OneM2M network.
- Gateway (GW): Connects different networks to enable seamless communication.

3 System requirements

3.1 Requirements for the system as a whole

3.1.1 Channels of system components communication

The consistency and the role of every component to be done, for each component to be connected and transferring the actions and getting the reactions through the system.

3.1.2 Requirements to the modes of system operation (normal mode (reliability), emergency mode)

3.1.3 Requirements to the system diagnostic

In order to diagnose the system, it must be monitored using the appropriate tools included in the relevant system software. The tools should provide an easy interface for viewing diagnostic events and monitoring the program execution process.

3.1.4 Perspective of modernization

The system software can be modified to newer versions, the microcontroller can also be replaced with an updated model. Additionally, the other components can be replaced with newer and better versions as time passes. The program code can also be modified to make room for additions of other components.

3.1.5 Requirement to the end users and their qualification

System administrators maintain the system in automatic or manual mode through management and monitoring. The minimum number of service personnel is one person.

3.1.6 Criteria of appliance

The system must be able to scale:

- By productivity
- By capacity of information process

Scaling capabilities must be provided by the basic software and hardware used.

3.1.7 Reliability requirements

The system must be operational and restored in the following situations:

- If a Model is presenting outdated Data, it must be updated as quickly as possible
- When there is a problem with the system operating the model, the system can be rebooted or trouble shoot for the model to remain whole. activated to restart the system. This restart can be all that the problem needs in order to start working properly.

3.1.8 Safety Requirements

The external elements of the technical measures of the system, which are under voltage, must have protection against accidental contact, and the technical measures themselves must have a zeroing or protective grounding GOST 12.1.030-81 and PUE. The power supply system must provide a protective switch during overloads and short circuits in the load circuits, as well as manual emergency shutdown. General fire safety requirements must comply with the standards for household electrical equipment. In the event of fire, no poisonous gasses or vapors should be produced. After disconnecting the power supply, ensure that all fire extinguishers can be used. Harmful factors should not exceed the standards of SanPiN 2.2.2./2.4.1340- 03 of 06/03/2003.

3.1.9 Requirements for operation, maintenance, repair and storage of system components

The microclimate in rooms with the corresponding hardware has to correspond to norms of an industrial microclimate (GOST 12.1.005-88).

For normal operation of the network it is necessary to support (according to GOST 23.865-85):

- air temperature in the range from + 15C to + 20C;
- relative humidity at 20 C in the range from 30% to 70%;
- atmospheric pressure 760 mm Hg.

The technical means used must be regularly maintained according to the requirements of the technical documents, but not less than once a year. Regular maintenance and testing of technical means should include maintenance and testing of all used means, including workstations, servers, cable systems and network equipment, and uninterrupted power supplies.

According to the test results of technical means, the reasons for the defects should be analysed and eliminated. The location of the premises and its equipment must prevent uncontrolled entry by outsiders and ensure the security of confidential documents located in these premises and technical means.

3.1.10 Requirements to standardization and unification

The OneM2M model can be used for multiple purposes and has important features

- It is light and energy efficient
- It is very versatile
- It is programmable and configurable
- It has great connectivity

3.2 Requirements for types of collateral

3.2.1 Requirements to the system's hardware (technical characteristics of each devices in the system)

3.2.2 Structure and Contest of design system

The composition and content of system design work includes:

- design and coordination of the technical task for the system;
- system design;
- writing an explanatory note;

- design of graphic material;
- defense of the qualifying paper.

4 Technical and economic indicators

The cost of development should not exceed 4000 UAH

The service life of the system should be at least 18,000 thousand hours. (2 years)

5 Stages of system design Num Stage

№	Name of the stage of performance of qualification work	Deadline
1	Development and approval of the technical task	29.12.2023
2	Analysis of the technical task	05.01.2024
3	Substantiation of possible technical solutions	11.01.2024
4	System design and implementation	15.01.2024
5	Testing of the designed system	17.01.2024
7	Occupational safety and health	18.01.2024
8	Registration of the qualifying paper	19.01.2024
9	Preliminary defense of the qualifying paper	20.01.2024
10	Defense of the qualifying paper	26.01.2024

Additional conditions for performance of qualification work

Changes and additions may be made to this technical task during the qualification work.