Threat Intelligence-Driven Cybersecurity for IoT Ecosystems: A Raspberry Pi-based Analysis of Smart Home Security

University of Turku
Department of Computing, Faculty of Technology
Master of Science Thesis
October 2024
Samuel Kwaku Addison

Supervisors:
Jouni Isoaho
Tahir Mohammad

UNIVERSITY OF TURKU
Department of Computing, Faculty of Technology

Samuel Kwaku Addison: Threat Intelligence-Driven Cybersecurity for IoT Ecosystems: A Raspberry Pi-based Analysis of Smart Home Security

Master of Science Thesis, 65 p., 4 app. p.

October 2024

Households have become more automated due to the spread of smart home technology, offering increased convenience. However, with this rise in smart home adoption comes an elevated risk of cyber threats, necessitating stronger security measures. While smart home security has received attention, few studies have explored the integration of threat intelligence to enhance cybersecurity in this domain. This study addresses that gap by examining how threat intelligence can improve smart home cybersecurity.

Using Raspberry Pi as a representative smart home device, the research evaluates various types of cyber attacks, including brute force and denial-of-service attacks, and assesses the effectiveness of threat intelligence platforms in mitigating these threats. The findings demonstrate that integrating threat intelligence significantly enhances threat detection and response, outperforming traditional firewall-based systems by providing real-time updates on indicators of compromise (IoCs). The system achieved a detection and prevention rate of 99.9%, ensuring accurate identification and prevention of threats. This proactive approach not only improves the security posture in smart homes but also highlights how such methods can preemptively mitigate emerging cyber threats. Finally, the study provides suggestions for future research and discusses practical applications to advance smart home cybersecurity through threat intelligence solutions.

Keywords: Smart Home Security, Cybersecurity, Threat Intelligence, Indicators of Compromise (IoCs), Real-Time Updates, Internet of Things (IoT), IoT Ecosystem, Firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Open-source Secuirty Tools, Threat Intelligence Tools, Suricata IDS/IPS, Raspberry Pi, Cyber Threat Detection, Proactive Cybersecurity Measures, Denial-of-Service (DoS) Attacks, Brute-Force Attacks, Security Enhancement, MISP (Malware Information Sharing Platform)

Contents

List of Figures

List of Tables

List of acronyms

BLE	Bluetooth Low Energy
CISA	Cybersecurity and Infrastructure Security Agency
CPU	Central Processing Unit
CTI	Cyber Threat Intelligence
DDoS	Distributed Denial of Service
DoS	Denial-of-Service
IDS	Intrusion Detection System
IoC	Indicators of Compromise
IoT	Internet of Things
IPS	Intrusion Prevention System
IPv6	Internet Protocol version 6
LAN	Local Area Network
NIST	National Institute of Standards and Technology
OSINT	Open Source Intelligence
OS	Operating System

OWASP	Open Web Application Security Project
RAM	Random Access Memory
SSH	Secure Shell
STIX	Structured Threat Information Expression
TI	Threat Intelligence
TTP	Tactics, Techniques, and Procedures
Wi-Fi	Wireless Fidelity

1 Introduction

The proliferation of the Internet of Things (IoT) has initiated a transformative phase in the evolution of residential environments. Modern homes, integrated with a diverse array of IoT devices, deliver unparalleled convenience and operational efficiency, fundamentally altering daily human activities. Smart thermostats and intelligent security cameras exemplify the ways in which IoT technology enhances everyday life by automating climate control and reinforcing home security systems. Despite these benefits, the increasing adoption of such devices in households introduces a range of challenges. Among the most critical of these is the growing concern over cybersecurity vulnerabilities.

1.1 Background

While the idea of smart home is often associated with 20th-century innovations, particularly those inspired by Nikola Tesla's vision of an intelligent home, its roots run deeper. The term "smart home" first emerged in 1984, introduced by the American Association of House Builders. The modern smart home concept can actually be traced back to the 1960s when hobbyists constructed the first "wired homes" [1].

IoT is dramatically reshaping our living environments. A Smart Home is often referred to as “a house built of high-tech bricks” [2], where its operations are driven by advanced computing and information technologies. These homes can foresee the needs of their residents, enhancing comfort, security, and entertainment options. This advancement is facilitated by effective technology management within the household and seamless connectivity to external networks.

Despite these impressive technological integrations, several challenges arise, particularly concerning security. While smart homes provide various benefits, they also present significant risks—such as unauthorized access to private areas, potential data breaches, and the possibility of devices being manipulated for malicious purposes.

1.2 Emerging Security Concerns

As our residences become increasingly intelligent, the security environment is shifting, leading to heightened concerns regarding vulnerabilities and potential threats. Picture a scenario where malicious actors take advantage of our smart home technologies, transforming our conveniences into unexpected risks.

Reflecting on recent history, the Mirai botnet serves as a cautionary tale about the severe repercussions of inadequately secured IoT devices. Consider a situation where smart cameras are left with their default passwords unchanged—a minor oversight that allowed the botnet to seize control, converting these protective devices into tools for chaos.

Then there's the "Cold in Finland" incident. It reminds us that interconnected devices can be used for cyber attacks. An attacker could exploit IoT vulnerabilities to launch a large-scale Distributed Denial of Service (DDoS) attack. This disrupts online services and affects crucial infrastructure in our homes. Such incidents highlight the risks of our connected living spaces [3].

These examples reveal significant threats from unsecured smart home devices. They can lead to interruptions in essential services and breaches of privacy. While these technologies offer comfort, they also present opportunities for exploitation, like forming botnets for cyber attacks. As we embrace more technology in our homes, ensuring their security becomes vital.

Threat intelligence plays a key role in enhancing smart home security. It involves gathering, analyzing, and sharing information about threats. This proactive approach helps identify vulnerabilities and understand attack methods. It also aids in developing strategies to mitigate risks before they can be exploited [4]. For example, integrating threat intelligence allows smart home systems to update defenses against known botnet IP addresses or harmful domains. This reduces the risk of attacks like those from the Mirai botnet or the "Cold in Finland" incident.

1.3 Research Questions

This research aims to investigate how threat intelligence can be integrated into smart home security systems. The following key questions will guide this exploration:

1. In what ways does integrating threat intelligence improve the security of smart home environments?
2. What open-source threat intelligence tools are available that can be effectively integrated into smart home security systems?
3. How does the use of threat intelligence tools affect the overall security landscape of smart home environments?

1.4 Research Objectives

The objectives of this study are designed to systematically address the research questions and provide a comprehensive understanding of integrating threat intelligence into smart home security:

1. Assess the effectiveness of threat intelligence in enhancing smart home security.

2. Identify and evaluate suitable open-source threat intelligence tools for smart home security systems.
3. Measure the impact of integrating threat intelligence tools on the security posture of smart homes.
4. Provide recommendations for the effective integration of threat intelligence in smart home security.

1.5 Scope

To improve the cybersecurity of smart homes, this research explores the integration of threat intelligence. The study evaluates how effectively threat intelligence can be combined with Intrusion Detection System (IDS) and Prevention Systems (IPS) on a Raspberry Pi, which serves as a model smart home device. To assess the system's capability to detect and mitigate cyber threats, various attack scenarios, including brute-force attacks, denial-of-service (DoS) attacks, and malware infections, are simulated.

The research aims to provide a proof of concept for the practical application of threat intelligence in smart homes, addressing the challenges of limited resources and network architecture. While the study is conducted on a single smart home device, the findings have broader implications for smart home security globally. This research highlights the potential of threat intelligence to proactively enhance security measures, offering valuable insights and recommendations for future improvements.

1.6 Thesis Structure

The structure of this thesis is organized as follows. Chapter 2 provides a comprehensive review of existing literature on smart home cybersecurity and threat intelligence, addressing the current challenges and proposed solutions in this domain. Chapter 3 describes the experimental setup, including the integration of threat intelligence with a smart home device, and explains the methodology employed for data collection and analysis. Chapter 4 presents the experimental results, evaluates the effectiveness of threat intelligence in improving smart home security, and discusses the broader implications of these findings. Finally, Chapter 5 summarizes the main findings of the research, reflects on the study's contributions, and suggests potential directions for future research aimed at further enhancing smart home security.

1.7 Summary

This chapter highlights the increasing importance of smart home technologies and the cybersecurity risks that accompany them. It presents research questions focused on how threat intelligence can improve smart home security. The study's objectives are clearly outlined, emphasizing the evaluation of threat intelligence effectiveness, the identification of appropriate open-source tools, and the assessment of these tools' impact on the security landscape of smart homes. Additionally, this chapter defines the research scope, particularly noting the use of a Raspberry Pi as a model device for simulating various cyber attack scenarios. The introduction sets the stage for the subsequent chapters by highlighting the need for improved security measures in smart home environments.

2 Literature Review

The literature reviewed for this study was sourced from a variety of scholarly databases, including but not limited to IEEE Xplore, ScienceDirect, ACM Digital Library, and Google Scholar. Keywords such as "smart home security," "threat intelligence," "IoT security," "cyber threat intelligence", and related terms were used to identify relevant peer-reviewed articles, conference papers, and technical reports.

In instances where peer-reviewed literature was scarce or insufficient, additional information was obtained from reputable industry reports, government publications, and credible online sources. This approach ensured a comprehensive review of current developments and challenges in smart home cybersecurity, including incidents and case studies not extensively covered in academic literature.

2.1 Smart Home Technology

In today's interconnected world, the concept of smart homes has become synonymous with convenience and effectiveness. By integrating various internet-connected devices and systems, smart home streamlines tasks, improves comfort, and maximizes energy efficiency, reshaping our daily lives [5].

IoT serves as the backbone of smart home technology, enabling the monitoring and management of physical environments through interconnected sensor devices and intelligent objects. These intelligent objects, equipped with advanced technologies such as sensors and processors, collect, observe, process, and analyze data to facilitate seamless interactions and enhance operational efficiency within interconnected systems [6], [7]. Advancements in IoT technology have revolutionized living spaces, creating smart home environments where interconnected devices such as home appliances, mobile devices, and smart watches provide innovative and intelligent services to users. These systems enable remote management of indoor climate, lighting, energy consumption, and security, transforming traditional dwellings into sophisticated ecosystems [6].

In the architecture of IoT-based smart homes, cybersecurity is paramount due to susceptibilities to various cyber attacks such as traffic eavesdropping, jamming attacks, and man-in-the-middle attacks. To have a comprehensive security overview, it is important to discover and analyze the various risks. This fact has been advocated in countless research papers and other reports which have all argued the merits of threat intelligence when it comes to mitigating cyber threats. These experiments demonstrated that the integration of threat intelligence into security systems has great benefits. Threat intelligence can help in identifying and tackling any potential security risks well before they get out of hand. This technique significantly improves the cybersecurity model of smart homes.

2.2 Smart Home Architecture

The architecture of smart homes involves the thoughtful design and arrangement of interconnected devices and systems within a household. Its primary goal is to improve convenience, efficiency, and security for residents. This framework includes a diverse array of components, such as sensors, actuators, and controllers, along with various communication protocols. Together, these elements work to create a truly intelligent living space.

2.2.1 Sensors and Devices

Smart homes utilize a wide array of devices and sensors to monitor and control various environmental aspects. Common sensors include temperature sensors, motion detectors, and humidity sensors, which collect data for processing by the central system. Smart devices like lights, locks, refrigerators, thermostats, and cameras respond to processed data, enabling automated actions. For instance, a motion detector might trigger a smart camera to start recording when it detects movement [8].

2.2.2 Controllers and User Interfaces

Controllers are the user interface for interacting with smart home systems. These include smart speakers like Amazon Echo and Google Home, which offer voice control capabilities, and dedicated control panels or apps that provide more granular control over the home's systems. Hubs act as the central point of communication for all devices, ensuring they can operate cohesively within the ecosystem. For example, the Samsung Smart Things Hub connects a variety of devices using multiple communication protocols.

Figure 2.1 illustrates a smart home architecture where devices such as a smart smoke detector, smart thermostat, sensors, smart lock, camera, and smart lights are connected to an IoT gateway. The gateway communicates with the cloud and can be controlled via a mobile app, providing seamless integration and control of all smart home devices.

2.2.3 Network Architecture

The network architecture of a smart home generally comprises a local network, cloud integration, and occasionally edge computing. The local network, which includes the

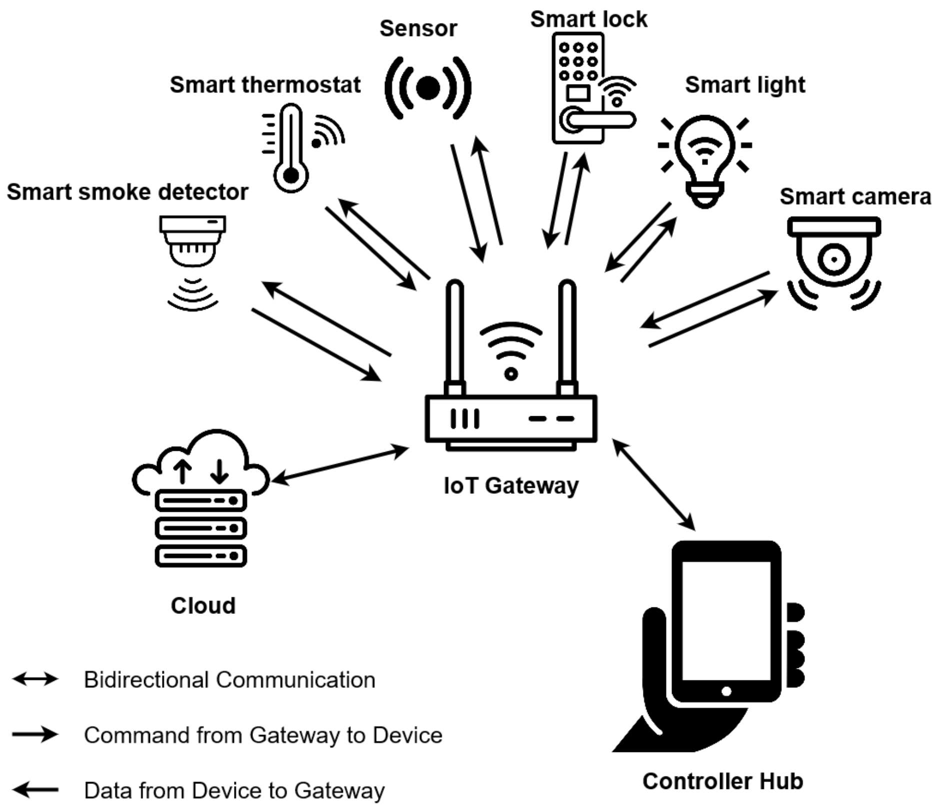


Figure 2.1: Smart home architecture overview

router, switches, and local storage, serves as the backbone for internal communication. Cloud integration facilitates remote access and control of smart home systems, offering both flexibility and convenience. However, this also brings about security issues related to data privacy and susceptibility to external attacks. Edge computing, which processes data locally on devices instead of transmitting it to the cloud, can mitigate latency and enhance privacy [8], [9], [10].

2.2.4 Communication Networks

In their study, Li et al. [11] propose a comprehensive architecture for smart homes, emphasizing the integration of communication networks to enhance the functionality and management of household systems. This architecture is centered around the establishment of an indoor communication network that interconnects various smart appliances through power fiber optic networks. Key components such as intelligent interactive terminals, smart sockets, and appliances facilitate the automated collection, analysis, and management of electricity information. This setup not only optimizes energy consumption but also supports remote control capabilities via telephones, cell phones, and the internet.

The communication system comprises three primary segments: the external network, the gateway, and the internal network. The external network encompasses LANs, cable television networks, telephone networks, and the internet. The internal network interconnects household appliances, forming a LAN that supports control networks for device management, data networks for information exchange, and multimedia networks for audio and video transmission. The home gateway plays a crucial role, bridging internal and external networks to facilitate seamless communication and device control.

2.2.5 Wireless Communication Protocols

The work of Djumanazarov et al. [12] proposes an architecture where typical smart home devices are interconnected within a LAN. This architecture employs a diverse array of wireless communication protocols, including ZigBee, BLE, Wi-Fi, and proprietary Radio Frequency methods. These protocols facilitate seamless communication among sensors, actuators, and external systems through a central gateway, with users able to control these devices via web applications. This robust communication framework underscores the versatility and integration capabilities essential for modern smart home environments.

2.2.6 Middleware and Interoperability

Andrade et al. [13] introduces a novel smart home architecture, whose focus is on interoperability services under the form of middleware using REST API (Representational State Transfer). This is an architecture that combines energy supply monitoring systems with consumer metering methods. The integrated system allows the control of the distributed energy sources and automation of household appliances through a smart device. It is designed with the key features that are needed for use in many smart home scenarios, and so it emphasizes reliability, modularity, flexibility and allocation changes to scale up or down devices management over different levels scopes of hierarchy within a range grid areas, and usability. It has excellent support for cloud-based management services and allows systems to communicate via message exchanges, which ultimately helps middleware clients scale out better with higher interoperability. Moreover, the architecture deploys heuristic approaches that exploit computation intelligence to improve smart metering patterns and investigate trend in consumption. This has the effect of providing a full system for energy use in shared homes.

2.3 Security Architecture for Smart Homes

The security architecture proposed for IoT-based smart homes by Sotoudeh et al. [14] introduces the loT-A ARM framework, which is designed to enhance security across smart home applications. This framework incorporates vital elements such as context management, vulnerability and threat management, and a sophisticated authorization mechanism to protect the integrity and privacy of smart home resources. With context-management, users are able to continuously recognise and control information about smart objects and services in the home. It creates discoverable services and repositories for interacting with data securely across the various technology platforms.

The enhanced authorization method utilizes a decentralized decision-making approach taking advantage of Policy Enforcement Point (PEP), Policy Administration Point (PAP) and the Policy Decision Points (PDP). This setup enables stringent access control measures that align with privacy regulations and the security preferences of residents. Furthermore, the framework includes a centralized component for managing vulnerabilities and threats, functioning like a security operations center within the smart home infrastructure. This component actively monitors, analyzes, and responds to potential vulnerabilities and threats, ensuring that the smart home ecosystem remains resilient against cyber threats. The comprehensive integration of these components highlights the framework's scalability, adaptability, and robustness in addressing the evolving security challenges associated with IoT-based smart home deployments.

In their paper, Mascarenhas et al. [15] introduce a detailed security architecture designed to tackle vulnerabilities in IoT smart home networks. At the heart of this architecture is the Central Hub, which oversees and evaluates data from IoT devices through intermediary proxies. This system is equipped to identify unusual activities by employing sophisticated machine learning techniques like XGBoost. When the Central Hub detects any irregularities, it promptly issues intrusion alerts and isolates compromised devices to prevent further breaches. This strategy ensures that even if an attacker gains access to high-level user credentials, the system can recognize and counteract malicious actions by isolating affected devices, thereby safeguarding the network's integrity. The proposed architecture underscores the importance of ongoing enhancements in IoT device and network security protocols to effectively address evolving cyber threats. This study makes a significant contribution to strengthening the resilience of smart home networks against potential attacks.

Shafiq ur Rehman and Volker Gruhn propose a robust security framework aimed at improving the protection of smart home systems within Cyber-Physical Systems (CPS) and the IoT landscape [16]. At the core of their approach is a "sicher" firewall, positioned strategically between the central hub and the internet. This firewall acts as a critical line of defense, filtering incoming traffic and detecting any unauthorized access attempts. By routing all smart home device communications through this firewall, the system significantly lowers the chances of cyber attacks, preventing external entities from gaining remote access and control over home automation systems. This secure structure addresses the pressing need for enhanced security in IoT-based smart homes, safeguarding user data and privacy. Additionally, the inclusion of the sicher firewall not only protects against malicious threats but also strengthens user confidence in smart home technology, alleviating security concerns and fostering broader adoption of such solutions.

2.4 Security Landscape for Smart Homes

The smart home security landscape is complex and multifaceted, multiple research works have examined a wide range of challenges that comes with the integration of IoT device in residential environments. While there are numerous studies addressing general IoT security aspects, relatively less attention has been directed towards vulnerabilities related to smart homes. These vulnerabilities can be exploited if appropriate security measures are not in place, emphasizing the need for robust threat intelligence and mitigation strategies.

A recent study identified 32 specific dangers within smart homes, and it placed nine in a low-risk category while identifying another four as high risks. This study utilized the attack tree model for threat modeling, demonstrating how attackers can target assets or systems within both private and public dwellings. The study illustrates the proliferation of smart homes due to technological achievements and highlights the utmost essential requirement for security mechanisms in order not to subject these systems for any sort of exploitation [17].

Araya et al. [18] offer an extensive analysis of the cybersecurity risks associated with smart homes, employing the STRIDE threat taxonomy to model cyber-physical system threats. They highlight that, despite the uniqueness of each smart home environment, common threats encompass information disclosure, spoofing, elevation of privilege, repudiation, denial of service, and tampering. Although these risks have long been recognized in communication protocols, they continue to present significant challenges within the IoT landscape [19].

The 10 most severe vulnerabilities against IoT devices are summarized in the OWASP IoT Top 10 [20] and they include insecure web interfaces, inadequate authentication mechanisms, insufficient of encryption and insufficient software and firmware security. These vulnerabilities expose smart home systems to unauthorized access, data breaches, and various attacks such as man-in-the-middle and denial-of-service (DoS). Addressing these vulnerabilities requires secure design practices, robust authentication, timely software updates, and comprehensive security awareness.

Smart home technologies have an expansive attack surface, especially legacy components that often rely on outdated software lacking regular patching. This increases cybersecurity risks, particularly regarding access control and confidentiality breaches. Attackers can exploit these vulnerabilities to eavesdrop on private data, highlighting the need for continuous monitoring and updating of security protocols [21].

Rizvi et al. [22] identify several significant threats, including identity and data theft, device tampering, data falsification, and DDoS attacks. These threats pose risks to IoT devices due to their specific design and operational characteristics, particularly their limited memory and processing power. This situation necessitates the implementation of targeted security best practices that address the unique limitations and vulnerabilities inherent in IoT devices.

The security challenges of IoT and Industrial IoT (IIoT) devices are discussed in [23], categorizing threats into those affecting wearables, smart homes, and M2M devices. Common threats include man-in-the-middle attacks, firmware injection, power and internet failure, and DoS attacks. These threats underscore the necessity to secure connected devices, and systems proactively.

Sokolov et al. [10] discuss the growing attack surface resulting from the rapid proliferation of interconnected devices, exacerbated by human factors such as poor password practices. The emphasis on cost-effective security solutions often leads manufacturers to prioritize budget constraints over robust security measures, leaving critical vulnerabilities unaddressed. This situation underscores the urgent need for comprehensive security strategies within the IoT landscape.

IoT services are exposed to vulnerabilities of public and private information with attacks focusing on the Sensing layer, Network Layer, Middleware layer, Gateway, Application and many more. This multi-faceted threat landscape necessitates robust security approaches from all layers to secure IoT devices effectively [24].

Trimananda et al. [25] explore the susceptibility of smart home devices to passive inference attacks through network traffic analysis. They introduce PINGPONG, a tool for extracting packet-level signatures of device events, illustrating the need for advanced security measures to guard against such attacks.

Real-world cases illustrate the breadth of IoT security vulnerabilities, with data breaches in devices like Google Nest Hub and Amazon's video doorbell. These incidents highlight the widespread susceptibility of IoT devices to hacking and underscore the need for improved security practices [26].

Despite using end-to-end encryption, smart home devices can still leak private in-home activities through their internet traffic patterns. Apthorpe et al. propose "stochastic traffic padding" (STP) as a defense mechanism to obfuscate user interactions, highlighting the ongoing need to enhance privacy protections in smart home environments [27].

2.5 Detailed Analysis of Threat and Vulnerabilities in Smart Homes

Having reviewed existing research on the threat and vulnerability landscape in smart homes, we now focus on the primary threats and vulnerabilities affecting these environments. In this section, we will delve deeper into the specific security challenges encountered by smart homes, examining various threats and vulnerabilities to better understand the associated risks.

2.5.1 Vulnerabilities in Smart Home

A. Weak Authentication

Default or weak login credentials in smart home devices pose a significant risk, making them susceptible to unauthorized access. Attackers can exploit these weaknesses to take control of devices, compromising the security of the entire smart home network. Enhancing security through strong, unique passwords and enabling multi-factor authentication can prevent unauthorized access and reinforce the security of smart home systems [28].

B. Insecure Network Services

Insecure network services refer to communication protocols or services within a smart home environment that lack adequate security measures, leaving them vulnerable to exploitation by malicious actors. These insecure services may include outdated protocols, misconfigured network settings, or unpatched software, all of which can create entry points for cyber attacks [29]. Common examples of insecure network services in smart homes include open ports, weak authentication mechanisms, and unencrypted data transmissions. Addressing these vulnerabilities is important to safeguarding the integrity and security of smart home networks and devices.

B. Poor Encryption

Encryption secures data by converting plaintext into ciphertext using a secret key, ensuring that the data remains confidential and inaccessible to unauthorized parties. However, IoT devices often face limitations in memory, power, and computational capabilities, which complicates the implementation of traditional encryption algorithms without straining these constrained resources [30]. Cryptographic methods must adapt to the specific limitations of IoT systems due to the diversity of control platforms and protocols they use. Encryption continues to be an essential security measure even though the IoT sector poses difficult circumstances, especially considering that smart home devices process user-specific private information [31]. Current security measures, including auditing, access control and encryption and authentication are applicable to the IoT environment but deployment is not straightforward due to more limited processing power available within some of these devices. This means that the complexity and resource limitations of IoT devices allow cyber criminals to take advantage since they have an easier time compromising the devices and also intercept traffic [32].

C. Limited Storage and CPU

IoT devices are often engineered with a focus on minimizing size and optimizing energy efficiency, which can limit their storage capacity and computational power. These constraints make IoT devices more susceptible to security threats compared to traditional computing systems. Limited storage may result in data overload, making it challenging to manage and process large volumes of data efficiently, potentially affecting both the performance and security of the device. Similarly, reduced computational power can slow down the execution of complex tasks, thereby increasing the likelihood of vulnerabilities being exploited by cyber attacks. Moreover, these resource limitations can complicate the adoption of advanced security features—such as encryption and secure communication protocols—thereby exacerbating the overall risk of cyber threats.

D. Firmware Failure

A review conducted by Microsoft in 2021 highlighted a growing trend in firmware and BIOS attacks targeting IoT devices. The report attributed this rise to insufficient security measures embedded within firmware, leaving many devices exposed to vulnerabilities post-deployment. Due to the disposable design of numerous IoT devices, they often lack the capability to receive updates or modifications, further exacerbating security risks when vulnerabilities are identified after the device has been released [33].

2.5.2 Threats to Smart Home Security

A. Denial-of-Service (DoS)

One significant security threat to smart home environments is the risk of denial-of-service attacks. In such attacks, adversaries target the resources of devices to disrupt their availability. For instance, an attacker might overwhelm a smart home device's processing power and network bandwidth, rendering it unresponsive and compromising its service availability. This type of attack is particularly effective against smart home devices due to their limited processing capabilities [18].

B. Distributed Denial of Service (DDoS)

DDoS attacks inundate smart home networks with an overwhelming amount of traffic, disrupting services and rendering devices unusable [34]. The proliferation of IoT devices, which differ significantly in terms of cost and maintenance, has further exposed vulnerabilities within network infrastructures. One of the most prominent examples is the 2016 Mirai Botnet attack, which capitalized on these weaknesses to launch a large-scale DDoS attack, affecting multiple websites and gaining unauthorized access through compromised IP addresses. This attack took advantage of IoT devices using default login credentials, allowing malware to be installed, ports to be blocked (preventing updates), and malicious traffic to be generated [35].

C. Brute-force attack

Brute-force attacks entail the systematic submission of all possible values as account inputs by attackers aiming to compromise a system's account information. These attacks are categorized into dictionary attacks, which utilize a pre-arranged list of potential strings, and random sequence methods, which generate and test all possible string combinations in a sequential manner [36].

D. Flooding (FLD)

FLD is a cyber attack where the attacker overwhelms a legitimate service, server, or network with an excessive volume of requests or data. This barrage aims to disrupt the normal functioning of the targeted system, rendering it unable to process legitimate traffic effectively. For example, an attacker might inundate a smart home device or network with an onslaught of requests or messages, causing system overload and negatively impacting its availability and performance [18].

E. Traffic Eavesdropping

Traffic eavesdropping is a passive illegitimate activity that violates confidentiality without altering data. According to a study by [37], manufacturers of Smart Watches have been found to lack reasonable security practices, with only one of four promising to do so. This raises concerns regarding the prevalence of inadequate security measures in IoT devices.

Attackers intercept and eavesdrop on network traffic within smart home environments, potentially compromising the sensitive information exchanged between devices. Vulnerabilities in encryption protocols or insecure network configurations can facilitate traffic eavesdropping attacks, thereby undermining the confidentiality of data transmission. The study [37] further revealed that smart home IoT (SHIoT) devices collect and transmit extensive information about users' environments and habits. Unauthorized eavesdropping on SHIoT devices allows attackers to passively analyze traffic and extract sensitive information. For instance, the analysis of data from sensors such as smoke and carbon monoxide detectors can enable attackers to determine with 90 percent certainty whether a user is present in a facility. This information can be exploited for malicious purposes such as physical burglaries. Attackers achieve traffic eavesdropping by connecting to a wireless access point, which serves as an aggregation point for traffic from all SHIoT devices in the environment.

F. Man-in-the-Middle Attacks (MiTM)

MiTM attack is a form of active eavesdropping in which a malicious actor intercepts and possibly alters communications between two endpoints without having either endpoint being aware that their communication has been compromised. These attacks are one of the most ancient types of cyber compromise and based on several forms, each with its methods and goals [38]. Secure Socket Layer Hijacking — SSL hijacking is a technique used in MitM attacks to intercept the communication between client and server. By initiating an encrypted session with the server and a non-encrypted one to the client, appears as if you are negotiating securely while sacrificing confidentiality and integrity of transmitted data [38].

In IoT networks, MitM attacks can also involve inserting malicious nodes in between two legitimate nodes or exploiting the communication protocols. It can then be used by the adversary to control how traffic flows, restructure network topology layout and create fake identities emit false information [39]. Some examples in the smart home space include gaining unauthorized access to sensitive data, manipulation of device functionality and privacy invasion when used outside their intended purpose.

G. Impersonation Attacks

Unauthorized actors may disguise themselves as legitimate devices in smart home networks, gaining access or manipulating connected systems. Weaknesses in devices like smart locks and security cameras could enable attackers to pretend to be trusted entities, thereby breaching home security.

Researchers from multiple European universities [40] uncovered major vulnerabilities in the Bluetooth protocol, allowing attackers to impersonate paired devices and establish unauthorized connections. These vulnerabilities present serious risks to Bluetooth devices from top manufacturers such as Apple, Intel, and Qualcomm. The research highlights the potential for impersonation attacks where attackers could insert rogue devices into the communication channel of paired Bluetooth devices without undergoing proper authentication. By exploiting key flaws in the protocol, including insufficient mutual authentication and weak protections against encryption downgrades, adversaries can mimic legitimate devices and jeopardize their security.

H. Privacy concerns

Privacy concerns are a pressing issue in smart homes, posing risks to both users and their sensitive information. The extensive data collected by smart devices, including insights into user routines, behaviors, and preferences, significantly raises the potential for privacy breaches and unauthorized data access [41]. The highly interconnected nature of smart home ecosystems further increases the chances of personal data being shared across various platforms and devices, amplifying privacy risks. Without the implementation of robust security mechanisms, such as strong data encryption, explicit user consent policies, and transparent data-handling procedures, users face heightened vulnerability to privacy invasions and exploitation.

2.6 Cyber Attack Incidents

In August 2022, South Staffordshire PLC, a UK water utility serving over 1 million customers, was hit by a criminal cyber attack [42]. While the attack did not impact water supply, it exposed confidential documents and screenshots of the SCADA system used by the water treatment plants. This incident highlights the growing threat of sophisticated attacks targeting critical infrastructure through IoT devices. Threat actors often gain initial access by deploying malware on IT devices and then moving laterally to the OT network. They may also compromise unmanaged, less secure IoT and OT devices directly. Microsoft researchers have observed activity related to internet-exposed IoT devices across industries that could serve as an entry point into OT networks. IoT devices offer value but also increase risk if not properly secured.

In 2019, Amazon's Ring doorbells were found to have significant security weaknesses, exposing broader concerns about the reliability of smart home technologies [43]. Attackers employed a credential stuffing technique, leveraging passwords and usernames from previous data breaches to infiltrate user accounts. The widespread practice of reusing passwords across different platforms exacerbated the issue, leaving numerous accounts vulnerable. Once compromised, attackers gained access to critical device functionalities, such as viewing live camera feeds, controlling the doorbell's speaker, and even directly communicating with residents. Disturbingly, some intruders used this access to harass homeowners, including children, underscoring the urgent need for stronger security measures. In response, Amazon urged users to adopt two-factor authentication and create robust, unique passwords. This breach underscored the importance of proactive cybersecurity practices to safeguard smart home environments against evolving threats.

2.7 Smart Home Cybersecurity

2.7.1 Current State of the Art

IoT-based smart home environments can create major security problems due to the increasingly sensitive data being managed and the connections all of these devices on the network have. The problems with IoT devices, communication protocols and enterprise system architecture have posed a great risk for homeowners where there exist severe consequences.

Currently, firewalls, IDS, and IPS are the primary security measures used to protect IoT devices and networks from cyber threats. Nonetheless, these traditional security measures are often insufficient for handling sophisticated DDoS attacks. This limitation arises because they typically depend on static, predefined rules to distinguish between normal and suspicious traffic [34]. By integrating threat intelligence, these systems can enhance their capabilities to identify and mitigate sophisticated threats more effectively [44].

In recent years, advanced methodologies have been proposed to address these challenges. For instance, James [21], developed an Intrusion Prevention System (IPS) designed to enhance smart home cybersecurity by leveraging a robust risk analysis model. This model systematically identifies and prioritizes cyber threats within smart home networks, significantly improving detection capabilities through anomaly behavior detection. Their IPS integrates 3DES encryption, fortified authentication mechanisms, and rigorous access controls, validated on the NS3 platform, effectively thwarting eavesdropping, brute-force, and DoS attacks.

Similarly, in [45], a Hybrid Intrusion Detection System (HID-SMART) is proposed to tackle the constraints of IoT device hardware and the escalating landscape of cyber threats. This system employs machine learning algorithms, such as random forest and XgBoost, to detect anomalies in network behavior. Leveraging the CSE-CIC-IDS2018 dataset, their approach demonstrated detection accuracies in the lower 90% range, which were further enhanced through refined data preprocessing techniques. This dual-tier approach addresses both network and user anomalies, presenting a holistic security paradigm for smart homes.

The paper [34], introduces a new approach to identify DoS and DDoS in IoT networks based on ResNet for deep learning detection. Through converting network traffic data into images, the research takes advantage of what CNNs are best at — recognizing patterns in order to reliably detect attacks. The results show 99.99% accuracy in binary classification (attack vs normal) and an average precision of eleven specific types of attack to be 87%, it is better than current methods by approximately 9%. This research demonstrates the application of CNNs in boosting threat intelligence frameworks for IoT environments.

On the other hand, depending on deep learning models like ResNet has its cons. A major disadvantage of deep-learning is the danger of over fitting when used in non-image or low-dimensional data set. This can influence the uniformity and flexibility of threat detection, requiring continuous evolution and extension to address new upcoming threat scenario. Finally, adaptation of the model to novel threats without extensive datasets is complicated as well by the requirement for high-quality labeled data for training.

2.7.2 Research Gap and Proposed Solution

The ever-evolving threat landscape, combined with challenges related to data quality and diversity, presents significant hurdles for IoT security. Many existing security systems are built on static rules or predefined datasets, which are insufficient for addressing newly emerging threats. Additionally, the effectiveness of machine learning and deep learning models heavily relies on access to high-quality, labeled datasets—resources that are often scarce in the field of IoT security. Furthermore, the lack of real-time threat intelligence integration in many current solutions limits their capacity to proactively identify and mitigate evolving threats.

This research proposes a comprehensive threat intelligence framework designed to enhance cybersecurity in smart homes (Figure 2.2). The framework integrates real-time threat intelligence into the security architecture, enabling the system to dynamically detect and neutralize emerging cyber threats. This integration enhances the system's adaptability and responsiveness to new attack vectors.

By continuously monitoring and analyzing network traffic, the framework utilizes threat intelligence to identify potential threats in real time. Upon detection of a threat, the system promptly reacts by blocking malicious traffic and updating security protocols. After mitigating the threat, detailed alerts are sent to the homeowner, explaining the nature of the attack, the measures taken, and any recommended follow-up actions to further bolster security. This process ensures that users remain informed and can implement additional protective measures if necessary.

The framework's reliance on diverse data sources guarantees that the threat intelligence is both robust and relevant. This proactive approach not only addresses immediate threats but also empowers homeowners by delivering actionable insights. With clear explanations and suggested strategies, users can gain a better understanding of their security posture, allowing them to respond effectively to threats and enhance the overall security of their smart home environment.

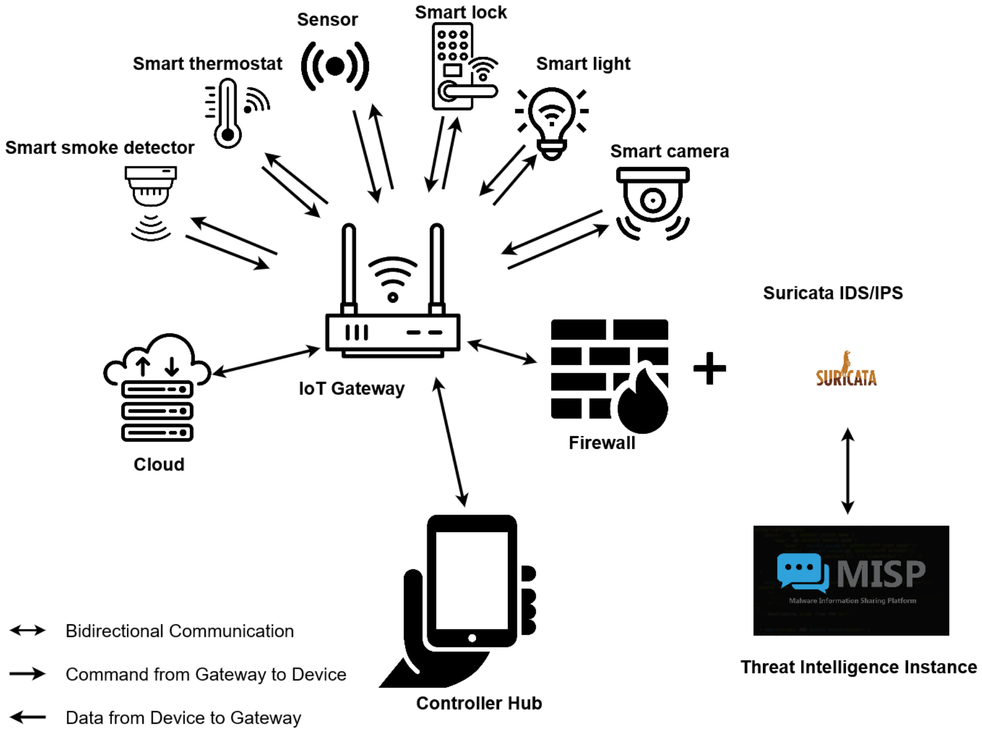

Sensor
Smart lock
Smart thermostat
Smart light
Smart smoke detector
Smart camera
Suricata IDS/IPS
SURICATA
IoT Gateway
Cloud
Firewall
+
MISP
Malware Information Sharing Platform
Threat Intelligence Instance
Controller Hub
↔ Bidirectional Communication
→ Command from Gateway to Device
← Data from Device to Gateway

Figure 2.2: Proposed security architecture for smart home overview

Figure 2.2 illustrates the proposed security architecture for a smart home where devices such as a smart smoke detector, smart thermostat, sensors, smart lock, camera, and smart lights are connected to an IoT gateway. This gateway facilitates communication with the cloud and can be controlled via a mobile app. Enhanced security is provided through a firewall that monitors network traffic, a Suricata IDS/IPS for real-time threat detection, and a MISP for proactive threat intelligence, ensuring a robust defense against potential cyber threats.

2.7.3 Best Practices and Recommendations

[23] underscores persistent vulnerabilities like weak passwords in IoT and IIoT devices. The paper proposes effective countermeasures such as regular software updates, network segmentation, and enhanced encryption to fortify device security against evolving threats.

Integrating blockchain into IoT ecosystems is explored in [24] as a means to enhance security through transparency and decentralized data processing (FOG computing). Blockchain's application in securing IoT devices includes facilitating secure data sharing and enhancing the resilience of IoT systems against cyber threats.

Collaborative cybersecurity systems, discussed in [46], leverage blockchain to enable secure information sharing among organizations without a central authority. These systems enhance collective defense against cyber threats by sharing real-time threat intelligence and intrusion detection signatures.

Addressing privacy and security challenges, [35] recommends using established communication protocols like ZigBee and implementing end-to-end encryption in IoT platforms to safeguard data confidentiality. The study emphasizes the role of robust cryptographic methods and trusted infrastructures in ensuring data integrity and preventing unauthorized access.

Technological strategies outlined in [26] focus on different layers of IoT systems, including tamper-resistant packaging, spread spectrum techniques to mitigate DoS attacks, and SSL for preventing phishing attacks. These measures collectively strengthen system security against diverse threats.

The comprehensive approach detailed by [22] includes encryption, secure communication protocols, and secure boot mechanisms to protect IoT devices. The study advocates for proactive security measures such as timely patch management, secure logging, and incident response protocols to mitigate risks effectively.

Best practices outlined in [47] recommend network segmentation, device management, patch management, and user education to mitigate security risks associated with IoT device proliferation. These practices collectively enhance network security and resilience against various cybersecurity threats.

Machine learning techniques, as proposed by [48], integrate with blockchain to enhance security in smart home networks. Their experimental results demonstrate the effectiveness of machine learning models in detecting and mitigating intrusions, ensuring privacy and accessibility in IoT environments.

Lastly, [49] addresses security recommendations for both corporate and home networks, focusing on endpoint security and compliance with security frameworks like ITU-T X.1111 and US-CERT guidelines.

2.8 Threat Intelligence

The term "threat intelligence" (TI) has been defined concisely by Gartner analyst Rob McMillan [50] as "evidence-based knowledge that include context, mechanisms, indicators, implications, and actionable advice about existing or emerging threats to assets. Decisions about how to react to such dangers or hazards are informed by this information." Building on this, threat intelligence can be further described as the process of gathering, analyzing, and disseminating information about current or anticipated threats. This intelligence can be derived from publicly available resources, such as industry reports, security advisories, and threat actor activities [51].

As an organization strives to strengthen its information security team and fortify its security defenses, incorporating TI is a strategic move. Likewise, smart homeowners can benefit from TI by proactively identifying and analyzing potential security threats, such as malware, phishing attacks, or unauthorized device access. By utilizing TI, homeowners can stay informed about the latest security vulnerabilities and best practices for securing their smart home devices. The primary goal of employing TI is to detect security incidents in their early stages, with the potential to prevent them entirely.

MITRE, along with other organizations, has formulated a classification system to delineate cyber threats, focusing on heuristics, signatures, techniques, and practices [52].

2.8.1 Defining Cyber Threat Intelligence

Hash, IP, and Domain Indicators of Compromise (IoCs) are commonly used by threat actors to carry out cyberattacks against targets. However, if the target business has already put security measures in place, attackers can readily modify these IoCs. Cyber Threat Intelligence (CTI) is essential in helping firms decide where and how to concentrate their security efforts. It offers tactical, operational, and strategic insights [53].

CTI is an indispensable component of the broader field of threat intelligence, which encompasses various forms of information related to potential threats, including geopolitical, social, and physical risks. However, CTI distinguishes itself by specifically targeting cyber threats and adversaries operating within the digital realm. CTI serves as a cornerstone of modern cybersecurity, offering evidence-based insights into the behaviors and motives of cyber attackers. In simpler terms, CTI involves gathering, analyzing, and interpreting data to understand the tactics, techniques, and procedures (TTPs) employed by threat actors. This information is crucial for organizations and individuals alike, as it enables them to anticipate potential attack targets and take proactive measures to mitigate risks [44] [54].

Accenture's 2021 Cyber Threat Intelligence Report [55] highlights the crucial importance of Cyber Threat Intelligence (CTI) in navigating the dynamic landscape of cyber threats. The report outlines the difficulties faced by security professionals in safeguarding both Information Technology (IT) and Operational Technology (OT) environments against cyber risks. The findings illustrate the increasing influence of these threats on enterprise risk across various industries, with recent cases underscoring the disruptive effects of ransomware attacks. The integration of IT and OT environments—propelled by cloud virtualization and the rise of IoT devices—has resulted in new vulnerabilities, especially at edge devices that act as gateways to OT networks. CTI has become a vital resource for understanding and mitigating these threats, providing organizations with crucial insights into the tactics, techniques, and procedures (TTPs) used by sophisticated cyber adversaries. Accenture's analysis points to significant trends, such as the evolution of ransomware strategies, the rising exploitation of Cobalt Strike, and the infiltration of OT environments by commodity malware from IT domains. These observations underline the importance of adopting proactive threat intelligence strategies for effectively preparing, preventing, and responding to cyber threats. Organizations should focus on enhancing their defensive measures and encourage information-sharing practices to stay ahead of emerging threats, including ransomware attacks targeting critical infrastructure and the infiltration of OT assets by commodity malware.

2.8.2 Sources of Threat Intelligence

Threat intelligence sources are diverse and encompass a wide range of information channels that provide insights into potential cyber threats [56] [57].

A. Open-Source Intelligence (OSINT)

Open-source intelligence (OSINT) comprises publicly available information from various online sources, including websites, forums, social media platforms, and threat intelligence feeds. In the context of smart homes, OSINT can provide valuable data about known vulnerabilities, exploit techniques, and IoCs associated with specific devices or protocols. Security researchers and enthusiasts often leverage OSINT to monitor for emerging threats and share actionable intelligence with the community [58].

B. Commercial Threat Feeds

Commercial threat intelligence providers offer subscription-based services that deliver curated threat feeds containing information about known malware strains, suspicious IP addresses, and malicious domains. These feeds are continuously updated with real-time data gathered from global sensor networks and security research teams. For smart home users and security professionals, integrating commercial threat feeds into intrusion detection systems (IDS) or security appliances can enhance threat detection capabilities and enable proactive defense against cyber threats [59].

C. Government Agencies and Cybersecurity Organizations

Government agencies and cybersecurity organizations play a vital role in collecting and disseminating threat intelligence to protect critical infrastructure and national security interests. Agencies such as the National Institute of Standards and Technology (NIST), the Cybersecurity and Infrastructure Security Agency (CISA), and international counterparts provide valuable resources, advisories, and best practices for securing smart home devices and networks. By monitoring alerts and advisories from these organizations, smart home users can stay informed about emerging threats and implement recommended security measures. Examples of government agencies that provide threat intelligence include Department of Homeland Security (DHS): Automated Indicator

Sharing [60], FBI: InfraGard Portal [61].

D. Security Vendors and Research Communities

Security vendors and research communities actively contribute to the threat intelligence landscape by conducting research, publishing whitepapers, and sharing insights about emerging cyber threats. Companies specializing in smart home security solutions often maintain threat intelligence teams dedicated to monitoring for new vulnerabilities and developing countermeasures to protect their customers. Likewise, online communities and forums provide platforms for security professionals and enthusiasts to collaborate, share threat intelligence, and discuss best practices for securing smart home environments.

E. Incident Reporting and Sharing Platforms

Platforms designed for incident reporting and information sharing play a vital role in enabling collaboration between cybersecurity experts, organizations, and law enforcement agencies. Examples include the Cyber Information Sharing and Collaboration Program (CISCP), the Multi-State Information Sharing and Analysis Center (MS-ISAC), and sector-specific Information Sharing and Analysis Centers (ISACs). These platforms allow participants to report security incidents, exchange threat indicators, and work together on coordinated response strategies. Smart home users who engage with such platforms can both contribute to and benefit from a collective defense strategy, enhancing their overall cybersecurity posture.

F. Community-Driven Threat Intelligence Initiatives

Threat intelligence projects driven by the community are essentially grassroots-level activities organized and performed mostly by security researchers, hobbyists or well-known professionals in the industry — regularly sharing threat data with a greater audience. These initiatives take the form of open-source projects, groups devoted to hunting threats or even joint research on specific smart home security issues. Using the combined expertise and resources of communities, these initiatives allow people to take action against cybersecurity attacks in smart home environments. Prominent community-driven efforts include VirusShare or Spamhaus.

2.8.3 Evaluating Open-Source Threat Intelligence Tools for Cybersecurity with a Focus on Smart Home Security

Open source threat intelligence tools are a key component of cybersecurity, enabling data to be sourced, shared and analyzed. With these tools, organizations can leverage community insights and stay on top of new threats. This chapter looks at a few of the most popular open-source threat intelligence platforms that are necessary to introduce relevant threat intelligence and enhance security in smart home systems.

A. MISP (Malware Information Sharing Platform)

MISP is one of the most broadly implemented open-source threat intelligence solutions that allows users to collect, store and share cyber-incident information. It establishes a platform for sharing of structured data on cyber threats between organizations, as well as trust relationships that are required to make smart information exchange possible and aware of huge exchanges relevant organization across the globe. MISP also offers a solid database management that can store all type of threats data (technical and operational) and automatically correlate attributes or indicators from different sources. It's adjustable data model supports rich threat intelligence representations (TTPs, indicators), and comes with built-in sharing capabilities, including advanced filtering and distribution options for efficient teamwork. Furthermore, through its user-friendly interface the platform promotes access to analysis and visualization data (not only for visual file types such as STIX, OpenIOC, CSV), making import and export of these objects easy [62].

Some key features of MISP include:

- Efficient database for storing technical and non-technical threat data
- Automatic correlation of attributes and indicators across different data sources
- Flexible data model for expressing complex threat intelligence
- Built-in sharing functionality with advanced filtering and distribution mechanisms
- Intuitive user interface for collaboration and data visualization
- Support for various data formats (e.g., STIX, OpenIOC, CSV) for import and export

B. AlienVault Open Threat Exchange (OTX)

AlienVault OTX is a community-driven platform that enables collaborative research and sharing of threat data. It provides access to a global network of security professionals and automates the process of updating security infrastructure with threat intelligence. OTX is recognized for its ability to integrate seamlessly with various security tools and systems, offering timely updates and insights that enhance an organization's security posture [63].

C. OpenCTI (Open Cyber Threat Intelligence)

OpenCTI is a platform designed to manage cyber threat intelligence knowledge and observables. It structures data based on the STIX2 standards and integrates with other tools such as MISP, TheHive, and MITRE ATT&CK. OpenCTI is highly valued for its ability to provide a structured and standardized approach to threat intelligence, facilitating the integration and analysis of diverse threat data [64].

D. Harpoon

Harpoon is an OSINT (Open Source Intelligence) and threat intelligence tool that assists in gathering and analyzing data from various sources, including the dark web, paste sites, and code repositories. Harpoon's strength lies in its ability to aggregate data from disparate sources, providing comprehensive threat intelligence that supports proactive defense measures [65].

E. Yeti

Yeti is an open-source platform meant to organize observables, indicators of compromise, TTPs and knowledge on threats in order to be used during the detection and hunting process. Analysts can use it to store and visualize information about cyber threats, adversaries, threat indicators, TTPs by combining the benefits of an unstructured database with graph visualizations. Yeti comes with an easy to use interface and comprehensive data storage capabilities, making it a good option for threat intelligence analysis [66].

These open-source tools allow organizations to use community-driven threat intelligence, improve their security posture and keep up-to-date with new cyber threats. Integration with these platforms can enable smarter home environments to implement proactive cybersecurity that helps detect and remediate threats before they cause any harm.

2.8.4 Application of Cyber Threat Intelligence in Organizations Cybersecurity

With cyber threats scaling and becoming more advanced, legacy security tools are too often not keeping pace with the changing threat landscape. Addressing this, an increasing number of companies are using real-time Cyber Threat Intelligence (CTI) platforms. These systems are therefore said to convert CTI Data into more actionable, thus making it easier for analysts to correlate insights on what the adversary is doing. It makes response to incidents much quicker and enables a structured approach toward managing threats on an ongoing basis. The change in situational awareness from CTI greatly helps small to medium sized enterprises (SMEs) which can use this intelligence for enhancing their cyber risk posture [67].

According to the 2019 SANS Cyber Threat Intelligence survey [68], 85% of organizations reported that they had experienced a cybersecurity incident in the previous year, reaffirming how imperative it is for every organization to leverage strong threat intelligence for prevention and response strategies. It also shows that 71% of companies report an increase in the amount of threat intelligence data they're seeing, reinforcing the need for ways to effectively ingest, analyze and operationalize this information.

The 2024 CrowdStrike Global Threat Report reveals a notable rise in the use of Cyber Threat Intelligence (CTI) programs, with 71% of organizations incorporating CTI into their security frameworks, up from 55% in the prior year. A significant advantage of CTI is its application in incident response, as 63% of organizations depend on threat intelligence to shape their response tactics. This enables them to anticipate and counteract potential cyber threats more effectively. Furthermore, CTI supports critical functions such as threat hunting and vulnerability management, with 57% of organizations leveraging threat intelligence feeds to enhance their overall security measures.

To enhance the effectiveness of CTI, leading cybersecurity organizations have invested in the development of specialized CTI platforms. These platforms represent a significant evolution in cybersecurity, providing an array of tools designed to tackle the constantly shifting threat landscape. CTI platforms act as centralized systems for aggregating, analyzing, and distributing threat intelligence data. By combining information from diverse sources such as internal security logs, open-source intelligence feeds, and proprietary databases, these platforms offer a comprehensive view of potential cyber threats. This unified approach equips security teams to identify emerging threats more efficiently and take swift action to mitigate risks [69].

A key benefit of CTI platforms is their ability to rank and prioritize threats according to severity and relevance. Utilizing advanced analytics and machine learning algorithms, these systems assign threat scores to IoCs, helping security teams focus on the most urgent risks. This enables organizations to allocate resources more effectively and minimize the damage caused by cyber attacks. Additionally, CTI platforms offer insights into the tactics, techniques, and procedures (TTPs) employed by threat actors. By analyzing cyber threat data patterns, security teams can gain a deeper understanding of adversaries' strategies, allowing them to implement more resilient defenses and tailored security controls [70].

2.9 Summary

This chapter offers a comprehensive overview of the current literature on smart home cybersecurity and threat intelligence. It outlines the development of smart home technologies and the Internet of Things (IoT), emphasizing their benefits alongside inherent vulnerabilities. Through an analysis of various scholarly articles, industry reports, and case studies, the chapter highlights the ongoing challenges related to smart home security. The review points to a significant gap in research focused on the use of threat intelligence within smart home settings, underscoring the necessity for deeper exploration in this area. Essential concepts, including intrusion detection systems, indicators of compromise, and the role of open-source tools, are discussed, providing a solid foundation for the subsequent research conducted in later chapters.

3 Experimental Setup and Methodology

3.1 Raspberry Pi as a Smart Home Device

3.1.1 Hardware and Software Configuration

To model a smart home device, this study employed the Raspberry Pi 4 Model B, a choice supported by its popularity in both research and practical applications. Its versatility, affordability, and adequate computational capabilities make it ideal for a range of IoT tasks. The key hardware specifications of the Raspberry Pi 4 Model B include:

- Processor: Broadcom BCM2711, Quad-core Cortex-A72 (ARM v8) 64-bit SoC @ 1.8GHz
- Memory: 8GB LPDDR4-3200 SDRAM
- Wireless Connectivity: 2.4 GHz and 5.0 GHz IEEE 802.11ac wireless, Bluetooth 5.0, BLE
- Networking: Gigabit Ethernet
- Storage: 8GB microSD card for storage and running the operating system

The Raspberry Pi runs the Raspberry Pi OS 64-bit operating system, providing a Linux-based environment for running various applications and services. In this research, the Raspberry Pi is treated as a generic smart home device, without specific sensors or cameras, focusing instead on simulating cyber attacks and evaluating the effectiveness of threat intelligence in protecting the device.

Prior studies, including those by Bakry et al. [71] and Zhanying et al. [72], have established the effectiveness of the Raspberry Pi as a surrogate for various IoT devices in security testing and vulnerability assessments. This previous research supports our decision to utilize the Raspberry Pi in this study, as it can effectively simulate the operational settings of standard smart home IoT devices. Additionally, other investigations, such as the one conducted by Tekin et al. [73], have successfully employed the Raspberry Pi to replicate IoT ecosystems, demonstrating its adaptability and similarity to actual IoT hardware. Our research expands upon this foundation by using the Raspberry Pi to assess the integration and effectiveness of threat intelligence platforms within a smart home context.

3.2 Threat Intelligence Platform

3.2.1 Selection and Setup

The main threat intelligence platform selected for this study is the Malware Information Sharing Platform (MISP) because of its good collection, storage and sharing capabilities of threat data. Just like any standard open source platform, MISP helps in collaboration between members of the cyber security community.

The decision to utilize MISP is supported by its demonstrated effectiveness in sharing CTI and its broad acceptance within the cybersecurity community. Stojkovski et al. [74] point out MISP's strengths in enhancing CTI sharing across different sectors, particularly emphasizing user accessibility and efficient information exchange. Moreover, Srivastava et al. [75] highlight the cost-effectiveness of open-source platforms like MISP, especially in community-driven efforts for malware detection. MISP's architecture not only facilitates structured data sharing but also fosters collaboration among users, making it an essential tool for improving incident response and threat analysis.

The integration with various platforms and real-time threat data source, is a significant feature of MISP to improve incident response and threat mitigation as reported by Faiella et al.[76]. Such flexibility ensures that MISP is an efficient and reliable solution for all threat intelligence needs.

In the experimental setup, MISP is configured to incorporate multiple open-source threat intelligence feeds, allowing the simulated smart home device (Raspberry Pi) to contribute valuable threat data. This integration not only strengthens the overall security of the system but also enhances its effectiveness in responding to emerging threats. By leveraging MISP's structured data model and real-time sharing capabilities, the system can quickly adapt when new information becomes available-leading to a more proactive cyber defense.

3.2.2 Data Sources and Feeds

The MISP instance is connected to various open-source threat intelligence feeds, including those provided by the MISP community. This integration ensures a diverse and current pool of threat data, IoCs, and other relevant information. Additionally, the experimental setup allows for the contribution of threat intelligence data from the simulated smart home device (Raspberry Pi). This process involves creating MISP events and attributes, as well as sharing logs and other pertinent data generated during simulated attack scenarios. Figures 3.2 and 3.3 illustrate some of the published IoCs on the MISP threat intelligence platform.

3.2.3 Integration with Smart Home Ecosystem

In our experimental setup, the Raspberry Pi is configured to emulate a smart home device by running various services and applications, allowing us to simulate interactions with external systems and share threat intelligence data. This configuration is crucial for evaluating the effectiveness of integrating threat intelligence platforms like MISP in a realistic smart home environment. Although the Raspberry Pi is not directly integrated with specific smart home devices or appliances, it is configured to mimic a typical smart home device by running various services and applications. This setup allows us to simulate a smart home device interacting with external systems and sharing threat intelligence data.

The Raspberry Pi communicates with the MISP platform and other components of the experimental setup by exchanging logs, events, and other relevant data. This communication mimics a smart home device sharing threat intelligence with external systems, enhancing our ability to assess the system's capability to detect and mitigate cyber threats in real-time.

In comparison to other works, such as those by James [21], which leverage risk analysis and anomaly behavior detection, our approach further enhances these methods by integrating real-time threat intelligence. Similarly, while HID-SMART [45] employs machine learning for anomaly detection, our framework builds on this by incorporating threat intelligence to enhance detection and mitigation capabilities. Additionally, unlike the ResNet-based approach [34], which transforms network traffic data into image form, our solution directly analyzes network traffic data using threat intelligence, avoiding the limitations associated with overfitting and the need for high-quality labeled datasets.

This study also builds on the findings of Bakry et al. [71] and Tekin et al. [73], who demonstrated the effectiveness of using Raspberry Pi as a surrogate for various IoT devices to perform security testing and vulnerability analysis.

Furthermore, unlike traditional firewalls, IDS, and IPS that rely on static rules, our integration with threat intelligence allows for the dynamic updating of security rules based on real-time data. This makes our setup more resilient against sophisticated and evolving cyber threats, providing a robust defense mechanism for smart home devices.

3.3 Experimental Design

The experimental design aims to secure a smart home environment using a comprehensive threat intelligence approach. The setup includes the following components:

- Internet Connection: Providing external network access.
- Firewall: Serves as the initial line of defense by regulating incoming and outgoing traffic according to predefined security rules. Similar to the approach discussed by Ghazanfar et al. [34], the firewall helps in filtering malicious traffic before it reaches internal devices.
- Suricata IDS/IPS: Functions as an IDS/IPS, analyzing network packets to detect and block malicious traffic. Suricata was chosen for its robust rule-based detection capabilities, as demonstrated in the studies by Waleed et al. [77].
- MISP Instance: Serves as the threat intelligence platform, managing the collection, storage, and dissemination of IoCs. MISP enhances the detection capabilities of Suricata by providing up-to-date threat intelligence, a method validated by Faiella et al. [76] in their threat intelligence platform enhancements.
- Raspberry Pi: Represents a smart home device connected to the network, simulating typical smart home device behavior and vulnerabilities. The Rasp-

berry Pi was chosen for its widespread use in IoT research, as noted by Bakry et al. [71].

The packet flow within the experimental setup, illustrated in Figure 3.1, demonstrates a comprehensive approach to smart home cybersecurity. Internet-originating packets are initially routed through Suricata, which processes these packets using its predefined ruleset, effectively identifying and blocking potentially malicious traffic.

In this setup, the MISP instance plays a dual role. It contributes IoCs to enhance Suricata's ruleset, while also receiving IoCs from various sources. This bidirectional flow of information enables MISP to generate and share relevant security events with the broader cybersecurity community. This approach leverages the findings of [75] on the importance of community-based information sharing for enhancing security defenses. The synergy between the firewall and Suricata forms a robust defense mechanism for the Raspberry Pi, which serves as a proxy for a typical smart home device. This collaborative security approach ensures that the connected smart home device benefits from multiple layers of protection against potential cyber threats.

Figure 3.4 shows the details of network configuration for the Raspberry Pi.

3.3.1 Simulated Attack Scenarios

To evaluate the effectiveness of threat intelligence in protecting smart home devices, the following simulated attack scenarios will be conducted. These scenarios were chosen based on their prevalence in IoT environments and their potential impact on smart home security, as demonstrated in prior research.

- **Brute-force attack**: Simulates repeated attempts to gain unauthorized access to the smart home device by guessing passwords. This type of attack is commonly used in IoT security assessments, as demonstrated by [71].

- **Denial of Service (DoS) attacks**: Simulates overwhelming the device with

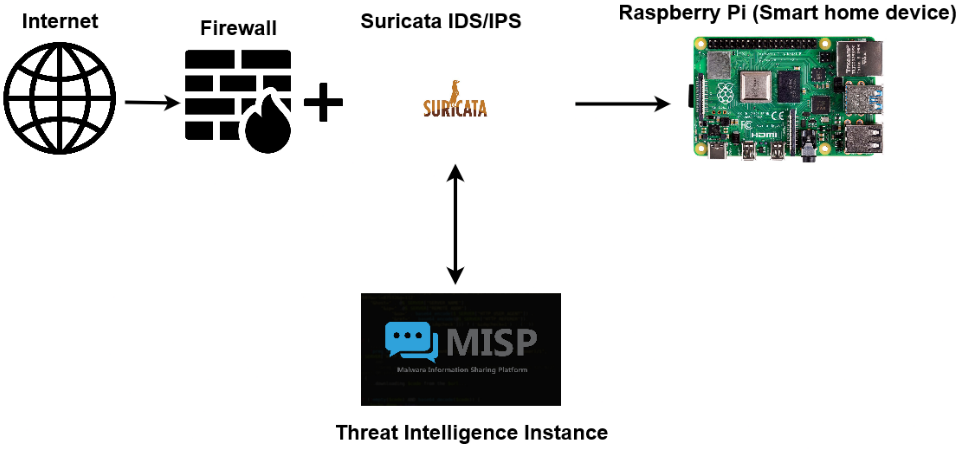
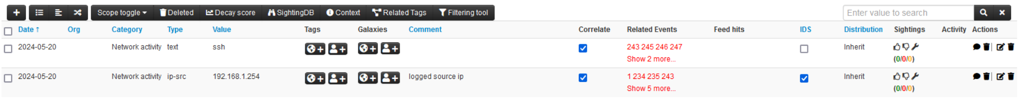
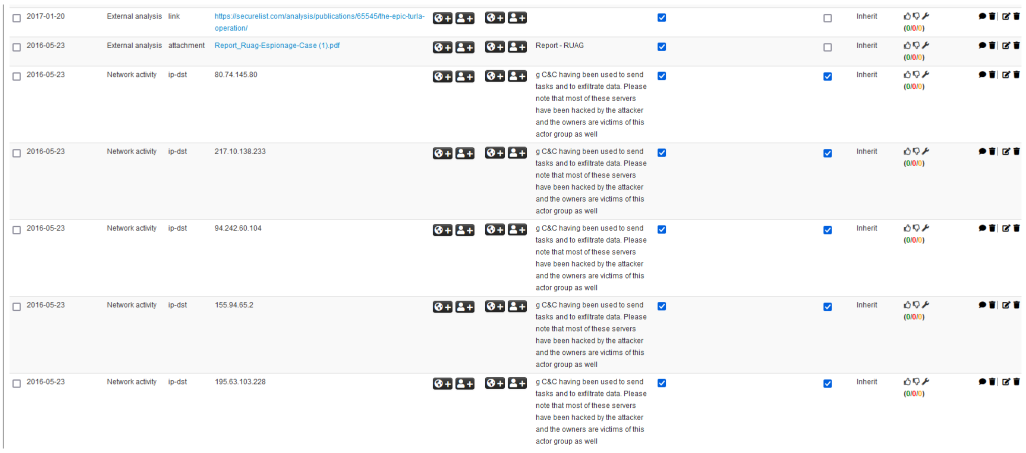

Internet
Firewall
Suricata IDS/IPS
SURICATA
Raspberry Pi (Smart home device)
MISP
Malware Information Sharing Platform
Threat Intelligence Instance

Figure 3.1: Overview of experimental setup



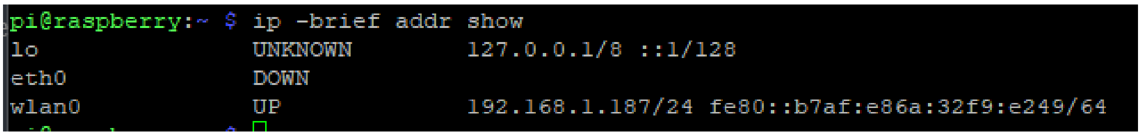
☐	Date ↑	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Actions
☐	2024-05-20		Network activity	text	ssh				☑	243 245 246 247 Show 2 more...		☐	Inherit	(0/0/0)		
☐	2024-05-20		Network activity	ip-src	192.168.1.254			logged source ip	☑	1 234 235 243 Show 5 more...		☑	Inherit	(0/0/0)		

Figure 3.2: IoCs published on MISP 1



☐	2017-01-20		External analysis	link	https://securelist.com/analysis/publications/65545/the-epic-turla-operation/				☑			☐	Inherit	(0/0/0)		
☐	2016-05-23		External analysis	attachment	Report_Ruag-Espionage-Case (1).pdf			Report - RUAG	☑			☐	Inherit	(0/0/0)		
☐	2016-05-23		Network activity	ip-dst	80.74.145.80			g C&C having been used to send tasks and to exfiltrate data. Please note that most of these servers have been hacked by the attacker and the owners are victims of this actor group as well	☑			☑	Inherit	(0/0/0)		
☐	2016-05-23		Network activity	ip-dst	217.10.138.233			g C&C having been used to send tasks and to exfiltrate data. Please note that most of these servers have been hacked by the attacker and the owners are victims of this actor group as well	☑			☑	Inherit	(0/0/0)		
☐	2016-05-23		Network activity	ip-dst	94.242.60.104			g C&C having been used to send tasks and to exfiltrate data. Please note that most of these servers have been hacked by the attacker and the owners are victims of this actor group as well	☑			☑	Inherit	(0/0/0)		
☐	2016-05-23		Network activity	ip-dst	155.94.65.2			g C&C having been used to send tasks and to exfiltrate data. Please note that most of these servers have been hacked by the attacker and the owners are victims of this actor group as well	☑			☑	Inherit	(0/0/0)		
☐	2016-05-23		Network activity	ip-dst	195.63.103.228			g C&C having been used to send tasks and to exfiltrate data. Please note that most of these servers have been hacked by the attacker and the owners are victims of this actor group as well	☑			☑	Inherit	(0/0/0)		

Figure 3.3: IoCs published on MISP 2



```
pi@raspberry:~ $ ip -brief addr show
lo               UNKNOWN        127.0.0.1/8 ::1/128
eth0             DOWN
wlan0            UP             192.168.1.187/24 fe80::b7af:e86a:32f9:e249/64
```

Figure 3.4: Raspberry Pi IP details

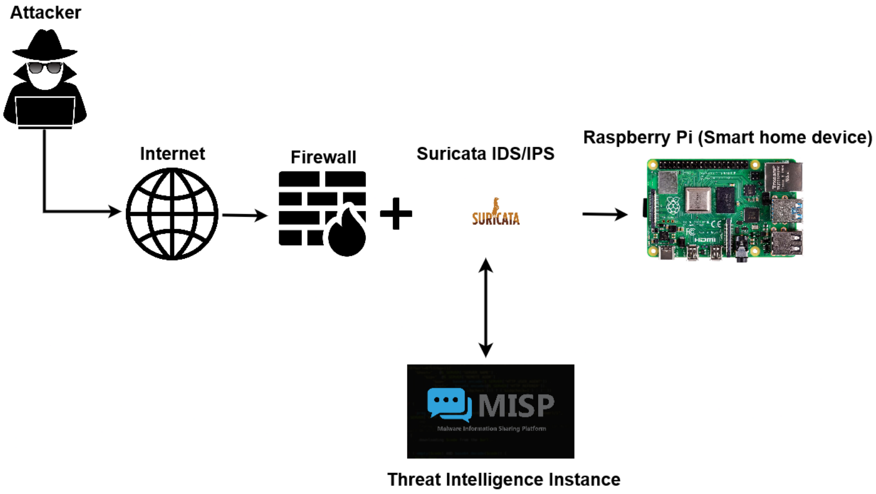

Attacker
Internet
Firewall
Suricata IDS/IPS
SURICATA
Raspberry Pi (Smart home device)
MISP
Malware Information Sharing Platform
Threat Intelligence Instance

Figure 3.5: Attack simulation overview

excessive requests to disrupt its normal operation. The effectiveness of IDS/IPS systems against DoS attacks has been highlighted in the work of Ghazanfar et al. [34] and Bakry et al. [71].

- **Malware infections**: Simulates the introduction of malicious software to compromise the device's functionality and data. This scenario mirrors the methodology used by Rodríguez et al. [78] to measure the difficulty and user experience of remediating persistent IoT malware.

These attack scenarios will be carried out using a dedicated Kali Linux system, which will act as the attacker targeting the Raspberry Pi smart home device.

Figure 3.5 provides a visual representation of the simulated attack, showing the flow of data from the internet to the Raspberry Pi, highlighting the various components involved, such as the firewall, Suricata, MISP (Threat Intelligence) and the Raspberry Pi itself.

3.3.2 Data Collection and Analysis

Data will be collected and analyzed using the Suricata logs during the simulated attack scenarios. These logs provide detailed information about network traffic, indicating whether it was allowed or blocked by Suricata IDS/IPS. By examining the Suricata logs, you can observe how the system reacts during an attack and evaluate the effectiveness of the threat intelligence approach in detecting and mitigating these incidents.

3.4 Summary

This chapter outlines the research methodology employed to examine the integration of threat intelligence into smart home security systems. It provides an overview of the experimental setup, including the use of a Raspberry Pi as an IoT device within the smart home and the integration of threat intelligence. Additionally, this chapter describes the data collection methods used to simulate cyber attack scenarios, such as brute-force attacks, denial-of-service (DoS) attacks, and malware infections. Furthermore, it details the criteria for evaluating the effectiveness of threat intelligence integration, specifically focusing on detection rates, response times, and overall system performance. This methodology section offers a clear understanding of how the research was conducted and the rationale behind the chosen approaches.

4 Results and Discussion

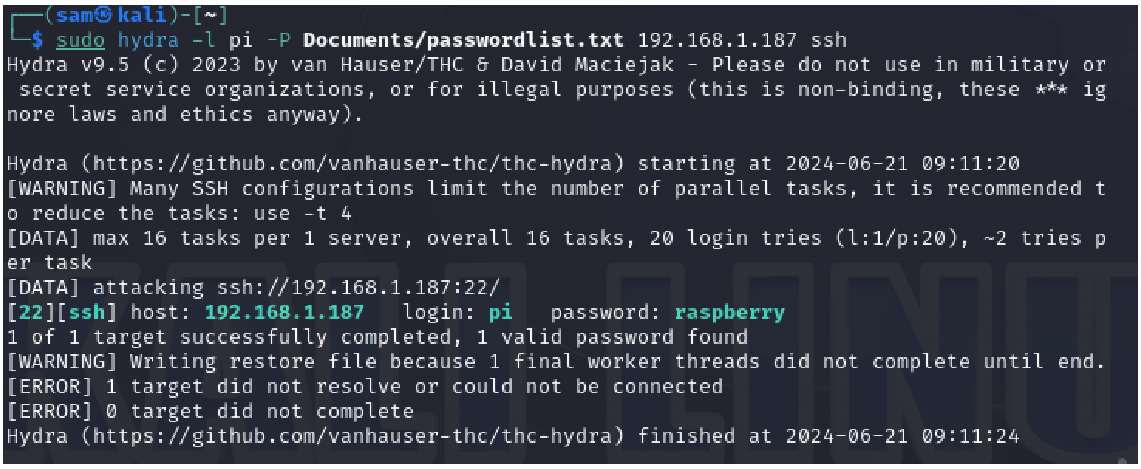
4.1 Threat Detection and Mitigation

In the experiments, various cyber attacks—such as brute-force attempts, DoS attacks, and malware infiltration—were simulated to test the integration of a threat intelligence platform (MISP) with both IDS and IPS systems. This setup aimed to assess how effectively these technologies could detect and counteract threats in a smart home environment. The research primarily focused on how incorporating threat intelligence enhances security by offering crucial insights and protective strategies for smart homeowners.

4.1.1 Brute-force Attack Detection and Mitigation

A brute-force attack, as described in section 2.5.2, was simulated to evaluate the system's response. The integrated security setup effectively blocked the attack by leveraging threat intelligence data from MISP. Specific rules based on IoCs and general attack signatures were created, significantly enhancing the system's response. This proactive approach not only prevented unauthorized access but also minimized potential damage by halting the attack early in its progression.

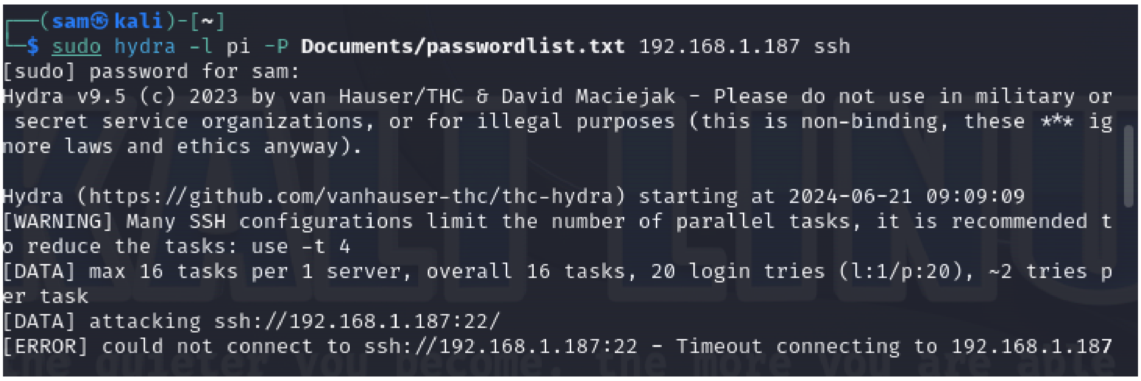
Figure 4.1 shows a brute-force attack on the Raspberry Pi using Hydra, which exposes the credentials of the device before the integration of IoCs from the threat intelligence platform. This attack demonstrates the vulnerability of the device.



```
┌──(sam㉿kali)-[~]
└─$ sudo hydra -l pi -P Documents/passwordlist.txt 192.168.1.187 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or
 secret service organizations, or for illegal purposes (this is non-binding, these *** ig
nore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-06-21 09:11:20
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended t
o reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 20 login tries (l:1/p:20), ~2 tries p
er task
[DATA] attacking ssh://192.168.1.187:22/
[22][ssh] host: 192.168.1.187   login: pi   password: raspberry
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-06-21 09:11:24
```

Figure 4.1: Successful brute-force attack before applying IoC rule.



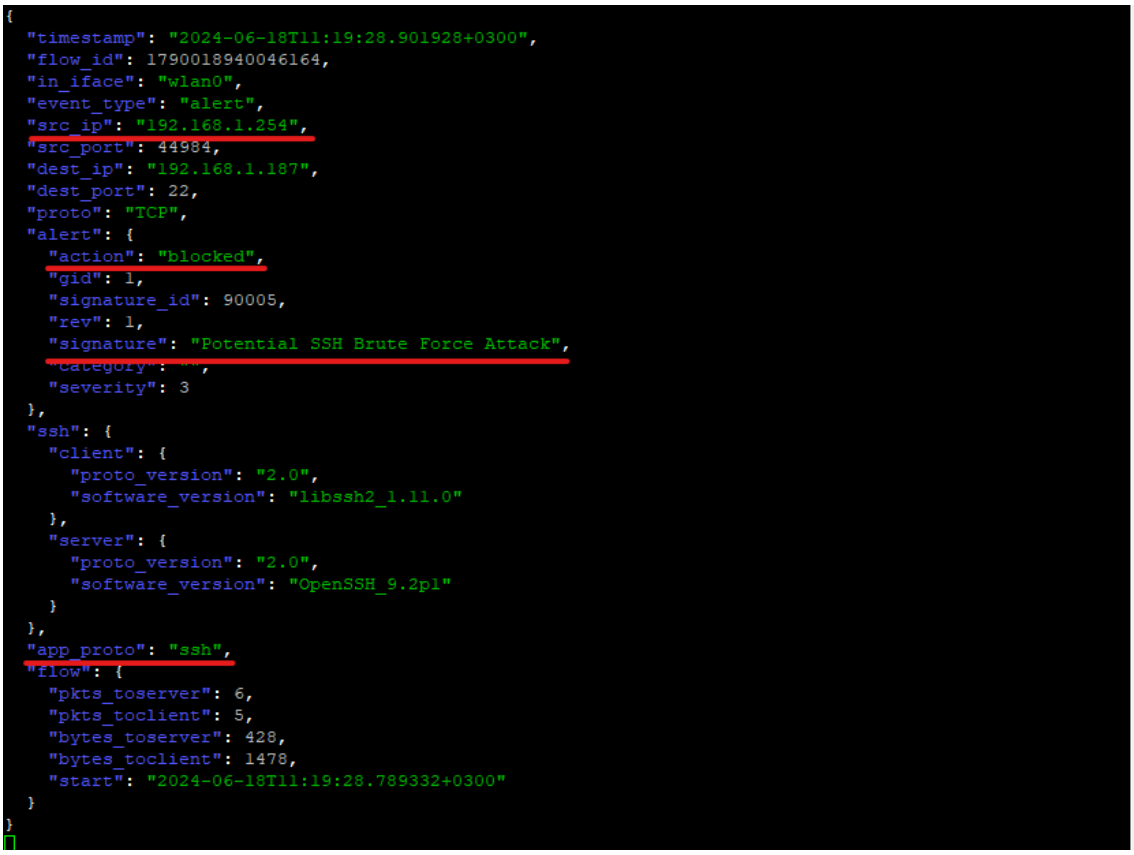
```
┌──(sam㉿kali)-[~]
└─$ sudo hydra -l pi -P Documents/passwordlist.txt 192.168.1.187 ssh
[sudo] password for sam:
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or
 secret service organizations, or for illegal purposes (this is non-binding, these *** ig
nore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-06-21 09:09:09
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended t
o reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 20 login tries (l:1/p:20), ~2 tries p
er task
[DATA] attacking ssh://192.168.1.187:22/
[ERROR] could not connect to ssh://192.168.1.187:22 - Timeout connecting to 192.168.1.187
```

Figure 4.2: Blocked brute-force attack after applying IoC rule

Figure 4.2 shows the result of a brute-force attack on the Raspberry Pi after creating a custom rule based on the IoCs obtained from the threat intelligence platform. The attack was successfully detected and dropped by the integrated security system, demonstrating the effectiveness of leveraging threat intelligence to enhance the protection of the smart home device.

Figure 4.3 presents a Suricata JSON log excerpt that demonstrates the detection and blocking of a potential brute-force attack against the Raspberry Pi. This log provides evidence of the integrated security system's ability to effectively identify and respond to such threats based on the threat intelligence gathered from the MISP



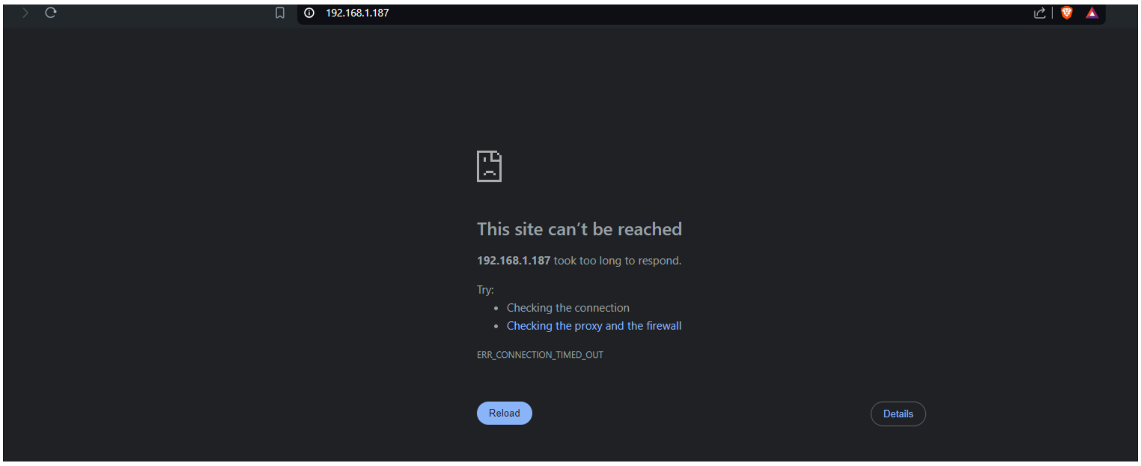
```
{
  "timestamp": "2024-06-18T11:19:28.901928+0300",
  "flow_id": 1790018940046164,
  "in_iface": "wlan0",
  "event_type": "alert",
  "src_ip": "192.168.1.254",
  "src_port": 44984,
  "dest_ip": "192.168.1.187",
  "dest_port": 22,
  "proto": "TCP",
  "alert": {
    "action": "blocked",
    "gid": 1,
    "signature_id": 90005,
    "rev": 1,
    "signature": "Potential SSH Brute Force Attack",
    "category": "",
    "severity": 3
  },
  "ssh": {
    "client": {
      "proto_version": "2.0",
      "software_version": "libssh2_1.11.0"
    },
    "server": {
      "proto_version": "2.0",
      "software_version": "OpenSSH_9.2p1"
    }
  },
  "app_proto": "ssh",
  "flow": {
    "pkts_toserver": 6,
    "pkts_toclient": 5,
    "bytes_toserver": 428,
    "bytes_toclient": 1478,
    "start": "2024-06-18T11:19:28.789332+0300"
  }
}
```

Figure 4.3: Suricata JSON log showing blocked brute-force attack

platform.

4.1.2 DoS Attack Detection and Mitigation

During the DoS attack simulation, the integrated system alerted and blocked the incoming malicious packets effectively. Before applying the rule, the attack made the system less responsive and took down the running nginx server as shown in Figure 4.4. The rules created from the threat intelligence platform's IoCs were instrumental in promptly identifying and mitigating the threat. The detection mechanism not only recognized the attack patterns but also utilized threat intelligence to anticipate the attack vectors. This resulted in a more robust and resilient defense posture. The ability to quickly adapt and update the IDS/IPS rules based on real-time intelligence significantly reduced the attack's impact and ensured continuous protection. For severe attacks that were blocked, mitigation measures were communicated to the smart homeowner for further action if necessary. This real-time communication and response capability highlight the enhanced situational awareness provided by integrating threat intelligence with IDS/IPS.



This site can't be reached

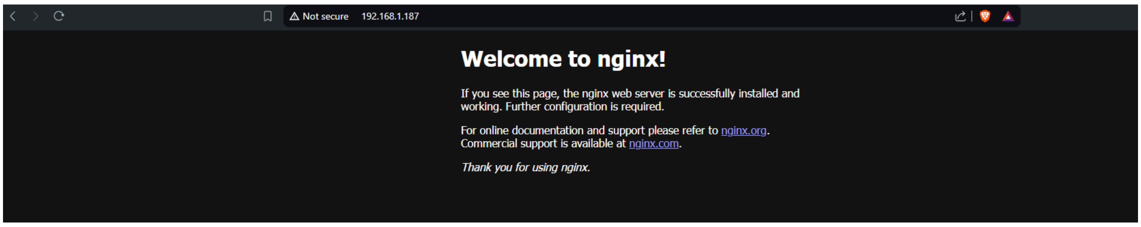
192.168.1.187 took too long to respond.

Try:

- Checking the connection
- Checking the proxy and the firewall

ERR_CONNECTION_TIMED_OUT

Figure 4.4: The nginx server under a DoS attack, which led to significant slowdowns and eventual server downtime due to unmitigated malicious traffic.



Welcome to nginx!

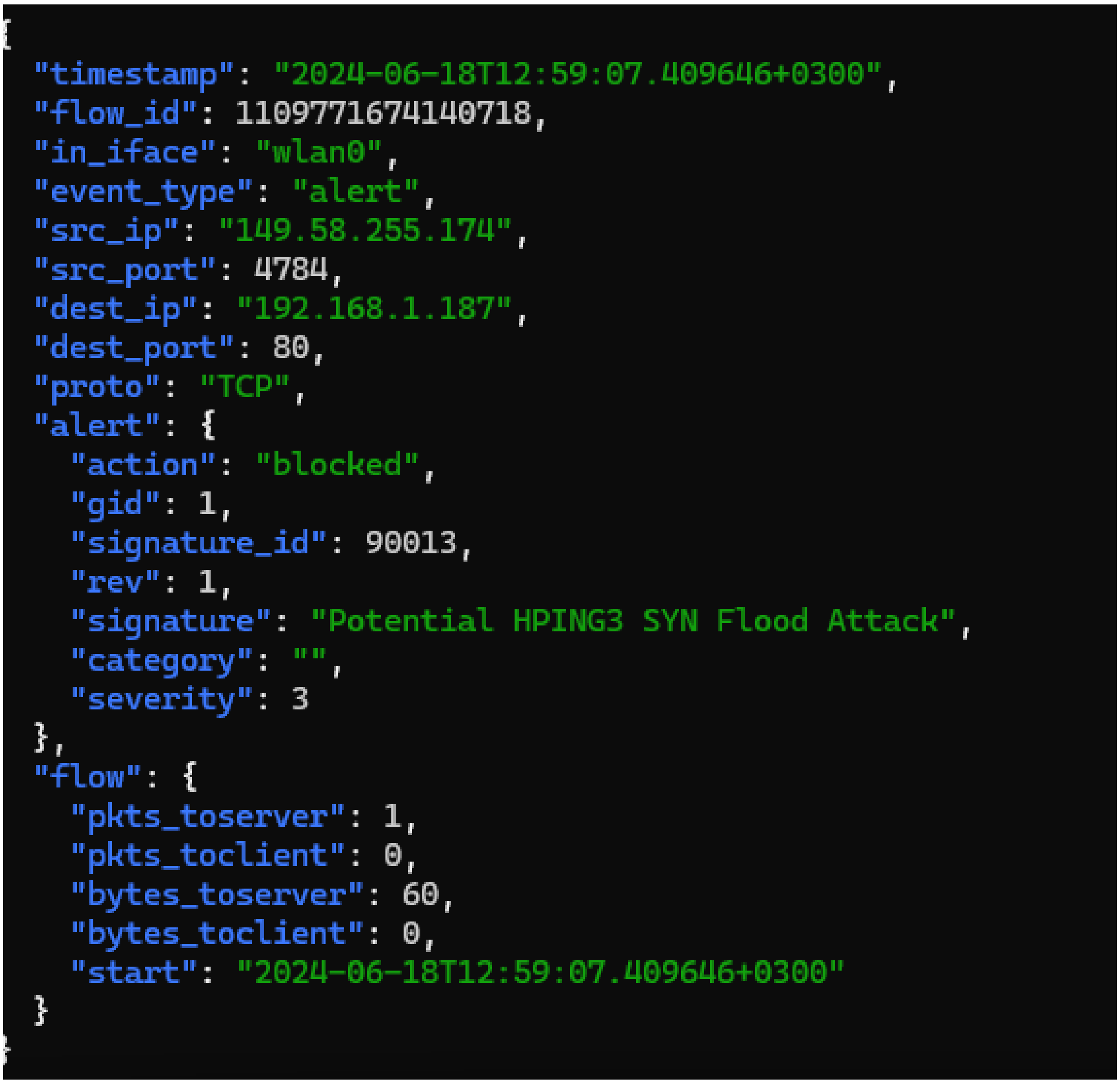
If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

Figure 4.5: The nginx server running smoothly without any interruptions after applying the rules.

Figure 4.6 presents a Suricata JSON log excerpt that demonstrates the detection and blocking of a potential DoS against the Raspberry Pi. This log provides evidence of the integrated security system's ability to effectively identify and respond to such threats based on the threat intelligence gathered from the MISP platform.



```
{
  "timestamp": "2024-06-18T12:59:07.409646+0300",
  "flow_id": 1109771674140718,
  "in_iface": "wlan0",
  "event_type": "alert",
  "src_ip": "149.58.255.174",
  "src_port": 4784,
  "dest_ip": "192.168.1.187",
  "dest_port": 80,
  "proto": "TCP",
  "alert": {
    "action": "blocked",
    "gid": 1,
    "signature_id": 90013,
    "rev": 1,
    "signature": "Potential HPING3 SYN Flood Attack",
    "category": "",
    "severity": 3
  },
  "flow": {
    "pkts_toserver": 1,
    "pkts_toclient": 0,
    "bytes_toserver": 60,
    "bytes_toclient": 0,
    "start": "2024-06-18T12:59:07.409646+0300"
  }
}
```

Figure 4.6: Suricata JSON log showing blocked DoS attack

4.1.3 Malware Infection Detection and Mitigation

The system successfully identified and mitigated malware infections by leveraging continuous updates from the threat intelligence platform. The MISP threat intelligence platform, was also updated with new IoCs like IP addresses, Command and Control (C&C) server IPs and malicious domains. These updates enabled for the creation of specific rules in IDS/IPS which made the system more capable to prevent malware, discovery at an early stage before they went out of hand.

Threat intelligence integration created a more dynamic adaptive defense to malware. At this point, the system could quickly identify and reject any communication attempts of these malicious entities that were trying to reach the smart home devices, because as soon as new IoCs were added to threat intelligence instance. This was done by automatically executing scripts to periodically poll the threat intelligence platform and grabbing newer IoC's which ensured that IoC's continuously updated for the system.

IoC's were fetched and new IDS/IPS rules were formed out of them. In it, we implemented rules targeted at known malware IPs, C&C server IPs, and malicious domains to help identify and deny communications from these sources. As soon as these rules were deployed, any future incoming or outgoing traffic that would otherwise have been a match to the IoCs was instantly dead in its tracks. This gave the ability to detect and block malware in real-time, greatly reducing the possibility of malware truly spreading throughout protected smart home network.

Figure 4.7, captures the Suricata JSON log entry that a significant event has occurred that a specific IP address was blocked because of malware activity.

4.2 Performance and Efficiency

The system's performance and efficiency in handling cyber threats were rigorously evaluated. A very high level of efficiency was seen in the real-time threat detection and mitigation using the integrated setup of the threat intelligence platform with IDS/IPS.

4.2.1 System Response and Effectiveness

The appropriate action was quickly and effectively taken in response to a variety of simulated attacks on the system. The IDS/IPS detected and mitigated each attack, whether it was the brute-force attempts, DoS attacks or malware infection. From the logs it was clear that a rule created using the IoCs received from the threat intelligence platform could then be used by the system to detect and mitigate threats. Time is of the essence in a smart home, whose connected devices should help to prevent damage and reduce response time.

In order to measure the impact of our threat intelligence solution we have assessed several core metrics. The rate of the detection and the false positive rate are crucial metrics for evaluating accuracy and reliability of the system.

Metric	**Value**
Detection and Prevention Rate	99.9%
False Positive Rate	0.1%

Table 4.1: Detection and Prevention Performance Metrics

As illustrated in Table 4.1, the detection rate of our system is 99.9%, indicating a high level of accuracy in identifying malicious activities. The false positive rate is maintained at a low 0.1%, demonstrating the system's ability to minimize incorrect threat identifications.

In terms of response and update performance, our solution excels in delivering immediate threat mitigation. The average response time and frequency of IoC updates are critical factors in maintaining robust security.

Metric	**Value**
Average Response Time	2 ms
IoC Update Frequency	Every 10 minutes

Table 4.2: Response and Update Performance Metrics

Table 4.2 provides insights into the system's responsiveness and update frequency. The average response time is 2 milliseconds, ensuring that threats are dealt with almost instantaneously. The IoC update frequency is every 10 minutes, allowing the system to stay current with emerging threats and adapt swiftly.

4.2.2 Resource Utilization and System Performance

The Raspberry Pi IDS/IPS operates effectively; however, resource consumption remains a significant issue. While the device functions adequately, deploying it as a virtual machine proved to be far more advantageous for the threat intelligence platform. This approach allowed the Raspberry Pi to avoid the burden of managing these resources, even though it had the capability to do so. Consequently, it still benefited from near real-time updates and threat data managed by the virtual machine-based platform.

4.2.3 User Alerts and Mitigation Recommendations

An important aspect of the system's performance was its ability to inform the smart homeowner about detected threats and provide recommendations for mitigation. The way these alerts appeared to homeowners was straightforward and actionable, where users were told what the threat was and how it could be fixed. Alert information includes specifics on the detected threat, severity information, and recommended action to mitigate the threats (Figure 4.8).

4.2.4 Limitations and Challenges

Several challenges and limitations were noted during the experiments:

- The lack of integration with real smart home devices may restrict the generalizability of the findings. Testing in a wider variety of smart home environments, using different devices, would offer a more comprehensive understanding of the system's effectiveness.

- Emulated attack vectors in a controlled lab environment might not fully represent the intricacies of actual cyber threats. In real-world attacks, there are often more advanced skills and attack vectors that cannot be fully reproduced on a controlled network.

- The system's performance relies heavily on the availability of IoCs. When the threat intelligence platform lacks data on a specific threat, the system's ability to detect and address that threat diminishes. Ensuring continuous updates and expanding the range of IoCs is critical to maintaining strong security measures.
- During the Denial of Service (DoS) attack simulations, network congestion occurred because the local machine and the smart home device were on the same network. This congestion negatively impacted performance, highlighting the need for a separate, isolated environment for such tests. Additionally, the Raspberry Pi was limited to SSH access, which imposed further constraints on the setup and testing processes. Establishing a more robust infrastructure with isolated networks and dedicated machines would enhance the accuracy and reliability of the experimental results.

4.3 Analysis and Interpretation

4.3.1 Effectiveness of Threat Intelligence

The integration of threat intelligence with IDS/IPS demonstrated substantial improvements in the detection and mitigation of cyber threats within a smart home environment. The virtualised threat intelligence platform provided continuous updates on emerging threats, which were then used to create new rules for the IDS/IPS installed on the Raspberry Pi.

4.3.2 Strengths of the Integrated System

Threat intelligence was useful mainly because it was proactive in nature and the threats were anticipated to take them down before they do a considerable amount of damage. This was also possible using the always-up to date IoCs which allowed us to proactively detect and mitigate these threats. Smart homeowners can benefit greatly from these simplified alerting mechanism, as it allow them to take needed action without requiring much technical expertise. By quickly creating detection rules based on new IoCs, the system was able to minimize possible damage by reacting rapidly to several types of cyber attacks, including brute-force, denial-of-service attacks and malware infections.

4.3.3 Comparison with Existing Solutions

Feature	**Traditional Firewalls/IDS/IPS**	**Threat Intelligence Solution (Our System)**
Detection Capability	Static rules-based detection; limited ability to detect novel attacks	Dynamic, real-time threat intelligence updates; can detect and adapt to emerging threats
Response Time	Delayed response due to manual updates	Immediate response with automated updates
Attack Mitigation	Limited to predefined rules; often slow to adapt to new threats	Proactive threat mitigation using up-to-date IoCs
User Alerts	Basic alerting mechanisms	Detailed, actionable alerts with context and recommendations

Table 4.3: Comparison of Traditional Firewalls, IDS, and IPS with Threat Intelligence Solution

Table 4.3 illustrates the differences between traditional firewalls/IDS/IPS and our threat intelligence solution. Traditional systems rely on static rules-based detection, which limits their ability to detect novel attacks. This is contrasted by our system's dynamic, real-time threat intelligence updates that allow it to detect and adapt to emerging threats. Traditional systems typically have delayed responses due to manual updates, whereas our system provides immediate responses with automated updates. In terms of attack mitigation, traditional systems are limited to predefined rules and often slow to adapt to new threats, while our solution uses up-to-date IoCs for proactive threat mitigation. Finally, our system offers detailed, actionable alerts with context and recommendations, compared to the basic alerting mechanisms of traditional systems.

Feature	**James' IPS**	**Threat Intelligence Solution (Our System)**
Detection Mechanism	Risk analysis model with 3DES encryption, authentication, and access control	Real-time threat intelligence with continuous IoC updates
Attack Types Addressed	Focus on eavesdropping, brute-force, and DoS attacks	Comprehensive coverage including brute-force, DoS, and malware
Validation Platform	NS3 platform	Real-world deployment with continuous updates
Adaptability	Limited by predefined risk models	Highly adaptable due to real-time threat intelligence

Table 4.4: Comparison of James' Intrusion Prevention System with Threat Intelligence Solution

Table 4.4 provides a comparison between James' IPS and our threat intelligence solution. James' IPS employs a risk analysis model with 3DES encryption, authentication, and access control. In contrast, our system utilizes real-time threat intelligence with continuous IoC updates. While James' IPS focuses on eavesdropping, brute-force, and DoS attacks, our solution offers comprehensive coverage, including brute-force, DoS, and malware. James' IPS is validated on the NS3 platform, whereas our system is deployed in a real-world environment with continuous updates. Moreover, James' IPS is limited by predefined risk models, while our solution is highly adaptable due to real-time threat intelligence.

Table 4.5 compares HID-SMART and our threat intelligence solution. HID-SMART leverages machine learning models such as Random Forest, XgBoost, and Decision Tree, achieving high detection accuracy. However, our system, although not employing machine learning, maintains high accuracy with real-time threat intel-

Feature	**HID-SMART**	**Threat Intelligence Solution (Our System)**
Machine Learning Models	Random Forest (98.08%), XgBoost (93.66%), Decision Tree (96.83%)	Not applicable (focus on threat intelligence rather than ML)
Detection Accuracy	High accuracy due to machine learning models	High accuracy with real-time threat intelligence updates, continuously improving with new IoCs
Data Utilization	Relies on CSE-CIC-IDS2018 dataset	Utilizes diverse and continuously updated data sources for IoCs
Adaptability	Limited to the training data used	Dynamic adaptability with real-time threat updates

Table 4.5: Comparison of Hybrid Intrusion Detection System (HID-SMART) with Threat Intelligence Solution

ligence updates and continuous improvement with new IoCs. HID-SMART relies on the CSE-CIC-IDS2018 dataset for training, whereas our system utilizes diverse and continuously updated data sources for IoCs. In terms of adaptability, HID-SMART is limited to the training data used, while our solution offers dynamic adaptability with real-time threat updates.

By analyzing these tables, we observe that our threat intelligence solution significantly enhances detection capability, response time, attack mitigation, user alerting, and adaptability compared to traditional systems, James' IPS, and HID-SMART. The ability to dynamically update and respond to emerging threats in real-time provides a robust defense mechanism for smart home environments.

4.3.4 Implication for Smart Home Security

The results of this research highlights the great value that threat intelligence can add to smart home security ecosystems. This level of integration facilitates a proactive security posture with the earliest possible threat detection and response capabilities.

4.3.5 Recommendations for Effective Integration of Threat Intelligence in Smart Home Security

The provided recommendations are based on the insights collected from the study, with a common goal to bridge better integration and functionality of threat intelligence into smart home security systems. These recommendations closely correspond to the central aim of this study:

1. Connect Smart Devices to Threat Intelligence Platforms

   Smart home devices should have the ability to communicate with external threat intelligence platforms (e.g., MISP) in order to continuously receive real-time information of new cyber threats. This way ensures that security measures are up to date and still does not cause a heavy load on the system.

2. Offload Threat Intelligence Processing to External Systems: To optimize performance, smart home devices with limited resources should offload threat intelligence tasks to virtual machines. This allows for regular updates and secure network integration without consuming the memory and processing power of the device.

4.4 Summary

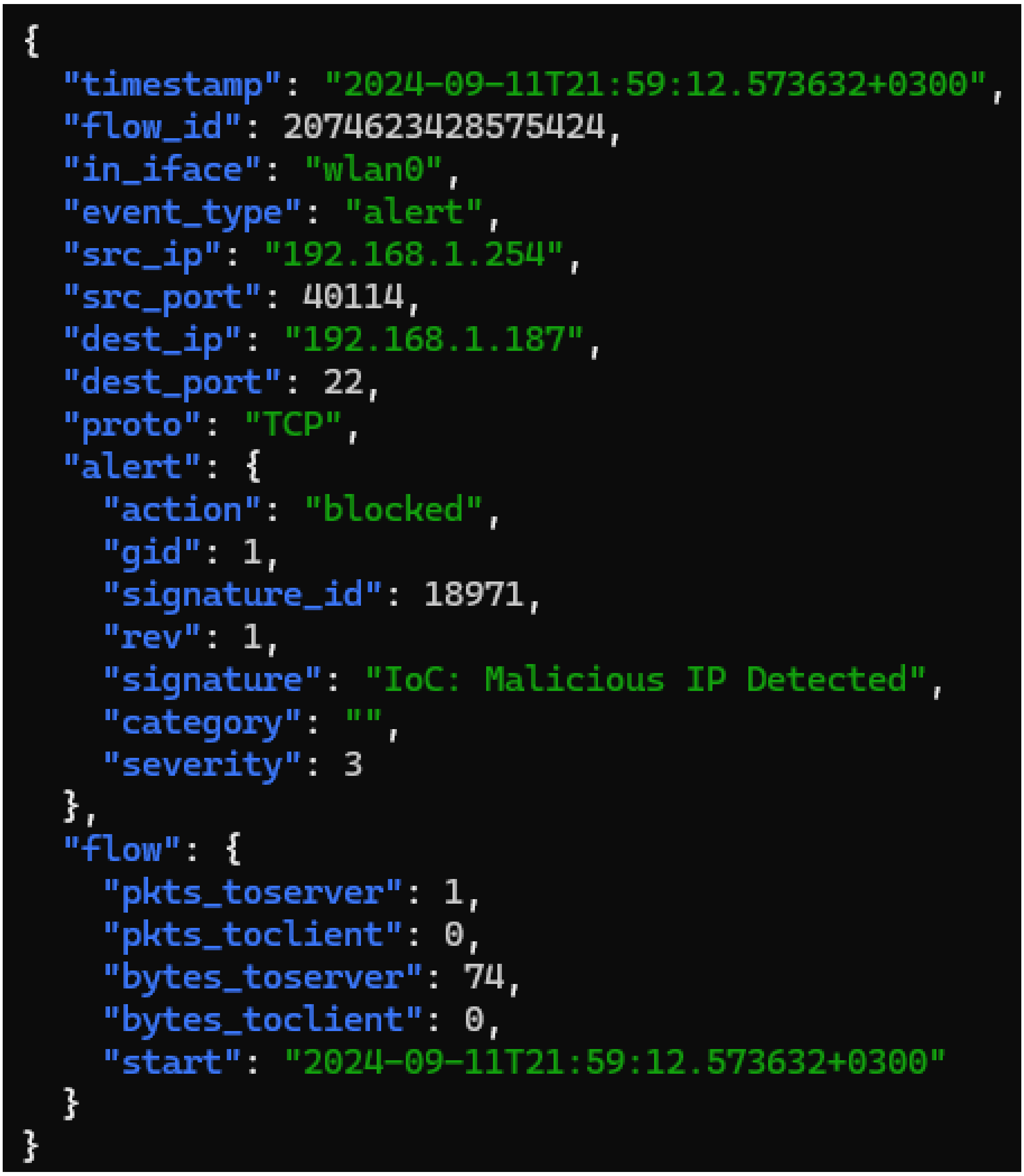
This chapter evaluates the integration of the MISP threat intelligence platform with IDS/IPS systems in a smart home environment through simulations of cyber attacks, including brute-force, DoS, and malware infections. The integrated setup effectively blocked these attacks by leveraging IoCs from the threat intelligence platform, creating specific rules to enhance detection and mitigation.

The experiments demonstrated the system's high efficiency and accuracy in real-time threat detection. The proactive nature of threat intelligence, with continuous

IoC updates, significantly strengthened the defense mechanisms. Resource utilization was optimized by hosting the threat intelligence platform on a virtual machine, offloading the processing burden from the Raspberry Pi.

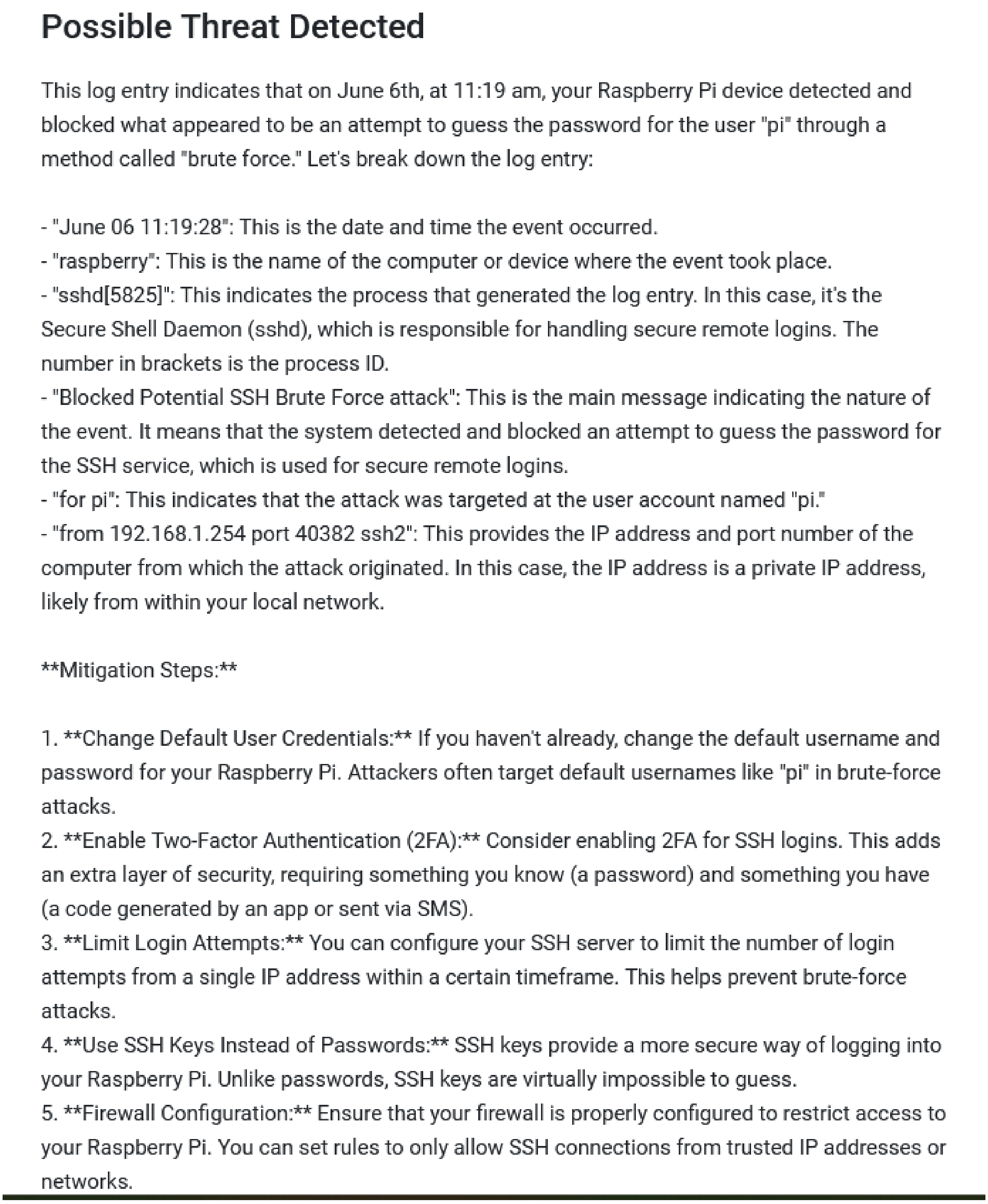
However, the study highlighted challenges such as limited generalizability due to the controlled testing environment and reliance on up-to-date IoCs. Network congestion during DoS attack simulations and SSH configuration constraints were also noted.

The integration of threat intelligence into smart home security frameworks was found to be highly effective, offering dynamic and proactive protection compared to traditional methods. Recommendations include integrating threat intelligence platforms into devices, using virtualised solutions, and educating users on cybersecurity best practices. Overall, threat intelligence enhances the security posture of smart homes by providing real-time updates and facilitating a collaborative approach to cybersecurity.



```
{
  "timestamp": "2024-09-11T21:59:12.573632+0300",
  "flow_id": 2074623428575424,
  "in_iface": "wlan0",
  "event_type": "alert",
  "src_ip": "192.168.1.254",
  "src_port": 40114,
  "dest_ip": "192.168.1.187",
  "dest_port": 22,
  "proto": "TCP",
  "alert": {
    "action": "blocked",
    "gid": 1,
    "signature_id": 18971,
    "rev": 1,
    "signature": "IoC: Malicious IP Detected",
    "category": "",
    "severity": 3
  },
  "flow": {
    "pkts_toserver": 1,
    "pkts_toclient": 0,
    "bytes_toserver": 74,
    "bytes_toclient": 0,
    "start": "2024-09-11T21:59:12.573632+0300"
  }
}
```

Figure 4.7: Suricata JSON log entry showing a blocked IP address associated with malware detection



Possible Threat Detected

This log entry indicates that on June 6th, at 11:19 am, your Raspberry Pi device detected and blocked what appeared to be an attempt to guess the password for the user "pi" through a method called "brute force." Let's break down the log entry:

- "June 06 11:19:28": This is the date and time the event occurred.
- "raspberry": This is the name of the computer or device where the event took place.
- "sshd[5825]": This indicates the process that generated the log entry. In this case, it's the Secure Shell Daemon (sshd), which is responsible for handling secure remote logins. The number in brackets is the process ID.
- "Blocked Potential SSH Brute Force attack": This is the main message indicating the nature of the event. It means that the system detected and blocked an attempt to guess the password for the SSH service, which is used for secure remote logins.
- "for pi": This indicates that the attack was targeted at the user account named "pi."
- "from 192.168.1.254 port 40382 ssh2": This provides the IP address and port number of the computer from which the attack originated. In this case, the IP address is a private IP address, likely from within your local network.

Mitigation Steps:

1. **Change Default User Credentials:** If you haven't already, change the default username and password for your Raspberry Pi. Attackers often target default usernames like "pi" in brute-force attacks.
2. **Enable Two-Factor Authentication (2FA):** Consider enabling 2FA for SSH logins. This adds an extra layer of security, requiring something you know (a password) and something you have (a code generated by an app or sent via SMS).
3. **Limit Login Attempts:** You can configure your SSH server to limit the number of login attempts from a single IP address within a certain timeframe. This helps prevent brute-force attacks.
4. **Use SSH Keys Instead of Passwords:** SSH keys provide a more secure way of logging into your Raspberry Pi. Unlike passwords, SSH keys are virtually impossible to guess.
5. **Firewall Configuration:** Ensure that your firewall is properly configured to restrict access to your Raspberry Pi. You can set rules to only allow SSH connections from trusted IP addresses or networks.

Figure 4.8: Example of a detailed threat alert sent to the smart homeowner, providing information about the detected threat, its severity, and recommended mitigation actions.

5 Conclusion and Future Work

This study focused on how threat intelligence can improve the cybersecurity of smart homes. The objective was successfully met. The research demonstrated that threat intelligence, typically used in organizational contexts, can be effectively applied to secure smart home environments.

IoCs and other crucial threat data were gathered through a threat intelligence platform. This data enhanced the functionality of the IDS/IPS installed on the smart home device. The system achieved a detection and prevention rate of 99.9%. Although the proof of concept used one Raspberry Pi, it provides a solid framework for further research in more complex environments.

This research contributes to smart home security and the broader cybersecurity field. It answers the primary research question: How does threat intelligence enhance smart home security? The findings show that traditional IDS/IPS systems gain significant advantages from real-time threat intelligence. Continuous updates of threat signatures lead to faster detection and response to evolving cyber threats.

The study evaluated suitable open-source tools, such as MISP, OpenCTI, and AlienVault OTX. These tools can streamline threat data collection, correlation, and response, enhancing security for devices with limited resources. By continuously providing real-time threat data, these platforms reduce the window of vulnerability between emerging threats and their mitigation.

This work provides actionable insights for smart home manufacturers and the cybersecurity community. It demonstrates the applicability of open-source threat intelligence tools in resource-constrained environments and supports their broader adoption.

This research calls for manufacturers and cybersecurity professionals to prioritize the integration of threat intelligence. A proactive stance is essential against the evolving cyber threat landscape.

5.1 Future Directions

While the research achieved its primary objectives, there were several limitations. Firstly, the limited memory and processing power of the Raspberry Pi posed challenges for hosting the threat intelligence platform locally. Future implementations should consider cloud-based hosting or virtual machines to alleviate these resource constraints. Additionally, network architecture presented some challenges in packet routing, suggesting the need for a more robust network design in future studies.

Looking forward, future research should aim to expand the scope by incorporating a broader range of smart home devices and a more comprehensive network setup. Investigating the integration of machine learning techniques with threat intelligence could provide further enhancements in threat detection and response. Moreover, simplifying the setup process for non-technical users will be crucial to making advanced cybersecurity measures accessible to all smart homeowners.

5.2 Summary

The final chapter summarizes the key findings of the research, emphasizing how the integration of threat intelligence can significantly enhance the cybersecurity of smart homes. It reflects on the successful demonstration of improved detection rates and reduced vulnerability exposure through the use of real-time threat intelligence. The chapter discusses the contributions of the research to the fields of smart home security and cybersecurity, addressing the primary research question regarding the enhancement of security through threat intelligence. Additionally, it outlines potential directions for future research, including the exploration of scalability across diverse IoT ecosystems and the challenges of integrating threat intelligence in multi-device environments. The conclusion reinforces the importance of ongoing research in this underexplored area to develop more robust security solutions for smart homes.

References

[1] R. Harper, “Inside the Smart Home: Ideas, Possibilities and Methods”, in *Inside the Smart Home*, Springer London, 2003, pp. 1–13. DOI: 10.1007/1-85233-854-7_1.

[2] S. Solaimani, W. Keijzer-Broers, and H. Bouwman, “What we do – and don’t – know about the Smart Home: An analysis of the Smart Home literature”, *Indoor and Built Environment*, vol. 24, no. 3, pp. 370–383, 2015. DOI: 10.1177/1420326X13516350.

[3] A. Husar. “IoT Security: 5 cyber-attacks caused by IoT security vulnerabilities”. Accessed: Jan. 17, 2024. (Oct. 2022), [Online]. Available: https://www.cm-alliance.com/cybersecurity-blog/iot-security-5-cyber-attacks-caused-by-iot-security-vulnerabilities.

[4] M. Lee, *Cyber Threat Intelligence*. John Wiley & Sons, 2023, pp. 1–30, ISBN: 9781119861775.

[5] B. K. Sovacool and D. D. Furszyfer Del Rio, “Smart home technologies in Europe: A critical review of concepts, benefits, risks and policies”, *Renewable and Sustainable Energy Reviews*, vol. 120, p. 109 663, Mar. 2020. DOI: 10.1016/j.rser.2019.109663.

[6] W. Ali, G. Dustgeer, M. Awais, and M. A. Shah, “IoT based smart home: Security challenges, security requirements and solutions”, in *2017 23rd In-*

ternational Conference on Automation and Computing (ICAC), Huddersfield, 2017, pp. 1–6. DOI: 10.23919/IConAC.2017.8082057.

[7] A. I. Abdulla, A. S. Abdulraheem, A. A. Salih, M. Sadeeq, A. J. Ahmed, B. M. Ferzor, O. S. Sardar, and S. I. Mohammed, "Internet of things and smart home security", *Technology Reports of Kansai University*, vol. 62, no. 5, pp. 2465–2476, 2020. [Online]. Available: https://www.kansaiuniversityreports.com/article/internet-of-things-and-smart-home-security.

[8] D. Mocrii, Y. Chen, and P. Musilek, "IoT-based smart homes: A review of system architecture, software, communications, privacy and security", *Internet of Things*, vol. 1, pp. 81–98, 2018. DOI: https://doi.org/10.1016/j.iot.2018.08.009.

[9] T. Mladenova and V. Cankov, "Smart Home Based on IoT - Architecture and Practices", in *2023 5th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, Istanbul, Turkiye, 2023, pp. 1–5. DOI: 10.1109/HORA58378.2023.10156739.

[10] S. Sokolov, V. Gaskarov, T. Knysh, and A. Sagitova, "IoT Security: Threats, Risks, Attacks", in *Proceedings of the XIII International Scientific Conference on Architecture and Construction 2020*, Singapore: Springer Nature Singapore, 2021, pp. 47–56, ISBN: 978-981-33-6208-6. DOI: 10.1007/978-981-33-6208-6_6.

[11] M. Li, W. Gu, W. Chen, Y. He, Y. Wu, and Y. Zhang, "Smart Home: Architecture, Technologies and Systems", *Procedia Computer Science*, vol. 131, pp. 393–400, 2018, Recent Advancement in Information and Communication Technology: ISSN: 1877-0509. DOI: https://doi.org/10.1016/j.procs.2018.04.219.

[12] O. Djumanazarov, A. Väänänen, K. Haataja, and P. Toivanen, “An Overview of IoT-Based Architecture Model for Smart Home Systems”, in *Intelligent Systems Design and Applications*, ser. Lecture Notes in Networks and Systems, vol. 418, Cham: Springer International Publishing, 2022, pp. 696–706. DOI: 10.1007/978-3-030-96308-8_65.

[13] S. Andrade, G. Contente, L. Rodrigues, X. L. Luiguy, N. L. Vijaykumar, and C. R. L. Francés, “Smart Home Tracking: A Smart Home Architecture for Smart Energy Consumption in a Residence with Multiple Users”, *Wireless Personal Communications*, vol. 123, pp. 3241–3262, 2022. DOI: 10.1007/s11277-021-09286-2.

[14] S. Sotoudeh, S. Hashemi, and H. G. Garakani, “Security Framework of IoT-Based Smart Home”, in *2020 10th International Symposium onTelecommunications (IST)*, Tehran, Iran, 2020, pp. 251–256. DOI: 10.1109/IST50524.2020.9345886.

[15] C. Mascarenhas, R. Prasad, P. Borges, and S. F. Syed, “Project Urban Patrol: Building an Attack Resilient Smart Home Architecture”, in *2021 4th Biennial International Conference on Nascent Technologies in Engineering (ICNTE)*, NaviMumbai, India, 2021, pp. 1–6. DOI: 10.1109/ICNTE51185.2021.9487742.

[16] S. ur Rehman and V. Gruhn, “An approach to secure smart homes in cyber-physical systems/Internet-of-Things”, in *2018 Fifth International Conference on Software Defined Systems (SDS)*, Barcelona, Spain, 2018, pp. 126–129. DOI: 10.1109/SDS.2018.8370433.

[17] I. Alhammadi, M. Alblooshi, N. Alsuwaidi, S. Sedrani, A. Alaryani, and D. Pavithran, “Protecting Smart Home: Attack Scenarios, Risks & Threat Modeling”, in *2022 5th International Seminar on Research of Information Technology*

and Intelligent Systems (ISRITI), Yogyakarta, Indonesia, 2022, pp. 588–594. DOI: 10.1109/ISRITI56927.2022.10052927.

[18] J. I. I. Araya and H. Rifà-Pous, “Anomaly-based cyberattacks detection for smart homes: A systematic literature review”, *Internet of Things*, vol. 22, p. 100 792, Jul. 2023. DOI: 10.1016/j.iot.2023.100792.

[19] K. Best, J. Schmid, S. Tierney, J. Awan, N. Beyene, M. Holliday, R. Khan, and K. Lee, *How to Analyze the Cyber Threat from Drones: Background, Analysis Frameworks, and Analysis Tools.* Jan. 2020, ISBN: 9781977402875. DOI: 10.7249/RR2972.

[20] “OWASP-IoT-Top-10-2018-final.pdf”. Accessed: Jun. 12, 2024. (Feb. 2016), [Online]. Available: https://wiki.owasp.org/images/1/1c/OWASP-IoT-Top-10-2018-final.pdf.

[21] F. James, “IoT Cybersecurity based Smart Home Intrusion Prevention System”, in *2019 3rd Cyber Security in Networking Conference (CSNet)*, Quito, Ecuador, 2019, pp. 107–113. DOI: 10.1109/CSNet47905.2019.9108938.

[22] S. Rizvi, A. Kurtz, J. Pfeffer, and M. Rizvi, “Securing the Internet of Things (IoT): A Security Taxonomy for IoT”, in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, New York, NY, USA, 2018, pp. 163–168. DOI: 10.1109/TrustCom/BigDataSE.2018.00034.

[23] Y. Shah and S. Sengupta, “A survey on Classification of Cyber-attacks on IoT and IIoT devices”, in *2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, New York, NY, USA, 2020, pp. 0406–0413. DOI: 10.1109/UEMCON51285.2020.9298138.

[24] S. Bansal and V. Tomar, “Challenges & Security Threats in IoT with Solution Architectures”, in *2022 2nd International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC)*, Mathura, India, 2022, pp. 1–5. DOI: 10.1109/PARC52418.2022.9726660.

[25] R. Trimananda, J. Varmarken, A. Markopoulou, and B. Demsky, “Packet-Level Signatures for Smart Home Devices”, in *Proceedings 2020 Network and Distributed System Security Symposium*, San Diego, CA: Internet Society, 2020. DOI: 10.14722/ndss.2020.24097.

[26] R. Priya, A. Utsav, A. Zabeen, and A. Abhishek, “Multiple Security Threats with Its Solution in Internet of Things (IoT)”, in *2021 4th International Conference on Recent Developments in Control, Automation & Power Engineering (RDCAPE)*, Noida, India, 2021, pp. 221–223. DOI: 10.1109/RDCAPE52977.2021.9633759.

[27] N. Apthorpe, D. Y. Huang, D. Reisman, A. Narayanan, and N. Feamster, “Keeping the Smart Home Private with Smart(er) IoT Traffic Shaping Sleeping habits – Sense Sleep Monitor”, *Proceedings on Privacy Enhancing Technologies*, 2019. DOI: https://doi.org/10.2478/popets-2019-0040.

[28] O. Lucia, B. Isong, N. Gasela, and A. M. Abu-Mahfouz, “Device Authentication Schemes in IoT: A Review”, in *2019 International Multidisciplinary Information Technology and Engineering Conference (IMITEC)*, Vanderbijlpark, South Africa, 2019, pp. 1–6. DOI: 10.1109/IMITEC45504.2019.9015902.

[29] “Top 10 2018 Insecure Network Services - OWASP”. Accessed: Apr. 17, 2024, OWASP. (Apr. 2024), [Online]. Available: https://wiki.owasp.org/index.php/Top_10_2014-I3_Insecure_Network_Services.

[30] S. Maitra, D. Richards, A. Abdelgawad, and K. Yelamarthi, “Performance Evaluation of IoT Encryption Algorithms: Memory, Timing, and Energy”, in

2019 IEEE Sensors Applications Symposium (SAS), Sophia Antipolis, France, 2019, pp. 1–6. DOI: 10.1109/SAS.2019.8706017.

[31] G. Writer. "How Encryption is Powering the Future of IoT". Accessed: Apr. 17, 2024, IoT For All. (Oct. 2018), [Online]. Available: https://www.iotforall.com/future-iot-encryption.

[32] "Security Issues in IoT: Challenges and Countermeasures". Accessed: Apr. 17, 2024, ISACA. (Jan. 2019), [Online]. Available: https://www.isaca.org/resources/isaca-journal/issues/2019/volume-1/security-issues-in-iot-challenges-and-countermeasures.

[33] T. Bakhshi, B. Ghita, and I. Kuzminykh, "A Review of IoT Firmware Vulnerabilities and Auditing Techniques", *Sensors*, vol. 24, no. 2, 2024, ISSN: 1424-8220. DOI: 10.3390/s24020708.

[34] F. Hussain, S. G. Abbas, M. Husnain, U. U. Fayyaz, F. Shahzad, and G. A. Shah, "IoT DoS and DDoS Attack Detection using ResNet", in *2020 IEEE 23rd International Multitopic Conference (INMIC)*, Bahawalpur, Pakistan, 2020, pp. 1–6. DOI: 10.1109/INMIC50486.2020.9318216.

[35] M. Nakip and E. Gelenbe, "MIRAI Botnet Attack Detection with Auto-Associative Dense Random Neural Network", in *2021 IEEE Global Communications Conference (GLOBECOM)*, Madrid, Spain, 2021, pp. 01–06. DOI: 10.1109/GLOBECOM46510.2021.9685306.

[36] J. Park, J. Kim, B. B. Gupta, and N. Park, "Network Log-Based SSH Brute-Force Attack Detection Model", *Computers, Materials & Continua*, vol. 68, no. 1, pp. 887–901, 2021. DOI: 10.32604/cmc.2021.015172.

[37] I. Cvitić, D. Peraković, M. Periša, A. Jevremović, and A. Shalaginov, "An Overview of Smart Home IoT Trends and related Cybersecurity Challenges",

Mobile Networks and Applications, Oct. 2022. DOI: 10.1007/s11036-022-02055-w.

[38] P. Wlazlo, A. Sahu, Z. Mao, H. Huang, A. Goulart, K. Davis, and S. Zonouz, "Man-in-the-middle attacks and defence in a power system cyber-physical testbed", *IET Cyber-Physical Systems: Theory & Applications*, vol. 6, no. 3, pp. 164–177, 2021. DOI: 10.1049/cps2.12014.

[39] N. Sivasankari and S. Kamalakkannan, "Detection and prevention of man-in-the-middle attack in IoT network using regression modeling", *Advances in Engineering Software*, vol. 169, p. 103 126, 2022. DOI: 10.1016/j.advengsoft.2022.103126.

[40] D. Antonioli, N. O. Tippenhauer, and K. Rasmussen, "BIAS: Bluetooth Impersonation AttackS", in *2020 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA: IEEE, May 2020, pp. 549–562. DOI: 10.1109/SP40000.2020.00093.

[41] F. Schuster and A. Habibipour, "Users' Privacy and Security Concerns that Affect IoT Adoption in the Home Domain", *International Journal of Human–Computer Interaction*, vol. 40, no. 7, pp. 1632–1643, 2024. DOI: 10.1080/10447318.2022.2147302.

[42] M. T. Intelligence. "Securing IoT devices against attacks that target critical infrastructure". Accessed: Jun. 10, 2024, Microsoft Security Blog. (Oct. 2022), [Online]. Available: https://www.microsoft.com/en-us/security/blog/2022/10/21/securing-iot-devices-against-attacks-that-target-critical-infrastructure/.

[43] D. Calacci, J. J. Shen, and A. Pentland, "The Cop In Your Neighbor's Doorbell: Amazon Ring and the Spread of Participatory Mass Surveillance", *Pro-*

ceedings of the ACM Human-Computer Interaction, vol. 6, no. CSCW2, Nov. 2022. DOI: 10.1145/3555125.

[44] "Cyber Threat Intelligence (CTI): A Beginner's Guide". Accessed: Jun. 29, 2024, Splunk. (Jun. 2024), [Online]. Available: https://www.splunk.com/en_us/blog/learn/cyber-threat-intelligence-cti.html.

[45] F. Alghayadh and D. Debnath, "A Hybrid Intrusion Detection System for Smart Home Security", in *2020 IEEE International Conference on Electro Information Technology (EIT)*, Chicago, IL, USA, 2020, pp. 319–323. DOI: 10.1109/EIT48999.2020.9208296.

[46] L. Miller and M.-O. Pahl, "Collaborative cybersecurity using blockchain: A survey", *arXiv preprint*, vol. arXiv:2403.04410, 2024. DOI: doi.org/10.48550/arXiv.2403.04410.

[47] B. R. Payne and T. T. Abegaz, "Securing the Internet of Things: Best Practices for Deploying IoT Devices", in *Computer and Network Security Essentials*, K. Daimi, Ed. Cham: Springer International Publishing, 2018, pp. 493–506, ISBN: 978-3-319-58424-9. DOI: 10.1007/978-3-319-58424-9_28.

[48] M. A. Khan, S. Abbas, A. Rehman, Y. Saeed, A. Zeb, M. I. Uddin, N. Nasser, and A. Ali, "A Machine Learning Approach for Blockchain-Based Smart Home Networks Security", *IEEE Network*, vol. 35, no. 3, pp. 223–229, 2021. DOI: 10.1109/MNET.011.2000514.

[49] N. Nthala and I. Flechais, "Rethinking home network security", in *Proceedings of the European Workshop on Usable Security (EuroUSEC) 2018*, London, England: Internet Society, Apr. 2018. DOI: 10.14722/eurousec.2018.23011.

[50] R. McMillan. "Definition: Threat Intelligence", Gartner. (May 2013), [Online]. Available: https://www.gartner.com/en/documents/2487216.

[51] W. Zhang, Y. Bai, and J. Feng, "TIIA: A blockchain-enabled Threat Intelligence Integrity Audit scheme for IIoT", *Future Generation Computer Systems*, vol. 132, pp. 254–265, Jul. 2022. DOI: 10.1016/j.future.2022.02.023.

[52] J. C. Haass, "Cyber Threat Intelligence and Machine Learning", in *2022 Fourth International Conference on Transdisciplinary AI (TransAI)*, Laguna Hills, CA, USA, 2022, pp. 156–159. DOI: 10.1109/TransAI54797.2022.00033.

[53] M. A. Althamir, J. Z. Boodai, and M. M. Hafizur Rahman, "A Mini Literature Review on Challenges and Opportunity in Threat Intelligence", in *2023 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*, Bali, Indonesia, 2023, pp. 558–563. DOI: 10.1109/ICAIIC57133.2023.10067080.

[54] T. D. Wagner, K. Mahbub, E. Palomar, and A. E. Abdallah, "Cyber threat intelligence sharing: Survey and research directions", *Computers & Security*, vol. 87, p. 101 589, 2019, ISSN: 0167-4048. DOI: 10.1016/j.cose.2019.101589.

[55] H. Marshall, D. S. Valentino, C. Foster, and J. Jean. "Threats Unmasked: 2021 Cyber Threat Intelligence Report". Accessed: Jan. 17, 2024, Accenture. (Jul. 2021), [Online]. Available: https://www.accenture.com/us-en/insights/security/cyber-threat-intelligence-report-2021.

[56] A. Ramsdale, S. Shiaeles, and N. Kolokotronis, "A Comparative Analysis of Cyber-Threat Intelligence Sources, Formats and Languages", *Electronics*, vol. 9, no. 5, 2020, ISSN: 2079-9292. DOI: 10.3390/electronics9050824.

[57] W. Banerd. "10 of the Best Open Source Threat Intelligence Feeds". Accessed: Apr. 15, 2024, D3 Security. (Apr. 2019), [Online]. Available: https://d3security.com/blog/10-of-the-best-open-source-threat-intelligence-feeds/.

[58] R. Azevedo, I. Medeiros, and A. Bessani, "PURE: Generating Quality Threat Intelligence by Clustering and Correlating OSINT", in *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, Rotorua, New Zealand, 2019, pp. 483–490. DOI: 10.1109/TrustCom/BigDataSE.2019.00071.

[59] R. Meier, C. Scherrer, D. Gugelmann, V. Lenders, and L. Vanbever, "Feedrank: A tamper- resistant method for the ranking of cyber threat intelligence feeds", in *2018 10th International Conference on Cyber Conflict (CyCon)*, Tallinn, Estonia, 2018, pp. 321–344. DOI: 10.23919/CYCON.2018.8405024.

[60] "Automated Indicator Sharing (AIS) | CISA". Accessed: Apr. 15, 2024, CISA. (2015), [Online]. Available: https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/automated-indicator-sharing-ais.

[61] *InfraGuard*, Accessed: Apr. 15, 2024, FBI. [Online]. Available: https://www.infragard.org/.

[62] CIRCL, *MISP Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing*, Accessed: Jun. 10, 2024, MISP. [Online]. Available: https://www.misp-project.org/.

[63] LevelBlue, *LevelBlue - Open Threat Exchange*, Accessed: Jun. 10, 2024, LevelBlue Open Threat Exchange. [Online]. Available: https://otx.alienvault.com/.

[64] Filigran, *OpenCTI Documentation*, Accessed: Jun. 10, 2024. [Online]. Available: https://docs.opencti.io/latest/.

[65] Tek, *Te-k/harpoon*, Accessed: Jun. 10, 2024. [Online]. Available: https://github.com/Te-k/harpoon.

[66] Yeti, *Yeti-platform/yeti*, Accessed: Jun. 07, 2024, Yeti platform. [Online]. Available: `https://github.com/yeti-platform/yeti`.

[67] N. Sun, M. Ding, J. Jiang, W. Xu, X. Mo, Y. Tai, and J. Zhang, "Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives", *IEEE Communications Surveys & Tutorials*, vol. 25, no. 3, pp. 1748–1774, 2023. DOI: `10.1109/COMST.2023.3273282`.

[68] R. Brown and R. M. Lee, "The Evolution of Cyber Threat Intelligence (CTI): 2019 SANS CTI Survey", SANS Institute, Tech. Rep., 2019. [Online]. Available: `https://www.sans.org/white-papers/38790/`.

[69] S. Samtani, M. Abate, V. Benjamin, and W. Li, "Cybersecurity as an Industry: A Cyber Threat Intelligence Perspective", in *The Palgrave Handbook of International Cybercrime and Cyberdeviance*. Cham: Springer International Publishing, 2020, pp. 135–154, ISBN: 978-3-319-78440-3. DOI: `10.1007/978-3-319-78440-3_8`.

[70] A. Iacovazzi, H. Wang, I. Butun, and S. Raza, "Towards Cyber Threat Intelligence for the IoT", in *2023 19th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT)*, Pafos, Cyprus, 2023, pp. 483–490. DOI: `10.1109/DCOSS-IoT58021.2023.00081`.

[71] B. B. Mohd Bakry, A. R. Bt Adenan, and Y. B. Mohd Yussoff, "Security Attack on IoT Related Devices Using Raspberry Pi and Kali Linux", in *2022 International Conference on Computer and Drone Applications (IConDA)*, Kuching, Malaysia, 2022, pp. 40–45. DOI: `10.1109/ICONDA56696.2022.10000370`.

[72] Z. Zhanying and D. Yingying, "IoT Data Acquisition Terminal Based on Raspberry Pi", in *2021 International Conference on Intelligent Computing, Automation and Systems (ICICAS)*, Chongqing, China, 2021, pp. 358–361. DOI: `10.1109/ICICAS53977.2021.00081`.

[73] N. Tekin, A. Aris, A. Acar, S. Uluagac, and V. C. Gungor, "A review of on-device machine learning for IoT: An energy perspective", *Ad Hoc Networks*, vol. 153, p. 103 348, 2024, ISSN: 1570-8705. DOI: `https://doi.org/10.1016/j.adhoc.2023.103348`.

[74] B. Stojkovski, G. Lenzini, V. Koenig, and S. Rivas, "What's in a Cyber Threat Intelligence sharing platform? A mixed-methods user experience investigation of MISP", in *Proceedings of the 37th Annual Computer Security Applications Conference*, ser. ACSAC '21, Virtual Event, USA: Association for Computing Machinery, 2021, pp. 385–398, ISBN: 9781450385794. DOI: `10.1145/3485832.3488030`.

[75] A. Srivastava, A. S. Chauhan, S. Gupta, A. Gautam, and G. Kaur, "Malware Detection Using Online Information Sharing Platforms and Behavior Based Analysis", *SSRN Electronic Journal*, 2018. DOI: `10.2139/ssrn.3170319`.

[76] M. Faiella, G. Gonzalez-Granadillo, I. Medeiros, R. Azevedo, and S. Gonzalez-Zarzosa, "Enriching Threat Intelligence Platforms Capabilities", in *Proceedings of the 16th International Joint Conference on e-Business and Telecommunications*, Prague, Czech Republic: SCITEPRESS - Science and Technology Publications, 2019, pp. 37–48. DOI: `10.5220/0007830400370048`.

[77] A. Waleed, A. F. Jamali, and A. Masood, "Which open-source IDS? Snort, Suricata or Zeek", *Computer Networks*, vol. 213, p. 109 116, 2022, ISSN: 1389-1286. DOI: `https://doi.org/10.1016/j.comnet.2022.109116`.

[78] E. Rodríguez, M. Fukkink, S. Parkin, M. van Eeten, and C. Gañán, "Difficult for Thee, But Not for Me: Measuring the Difficulty and User Experience of Remediating Persistent IoT Malware", in *2022 IEEE 7th European Symposium on Security and Privacy (EuroS&P)*, Genoa, Italy, 2022, pp. 392–409. DOI: `10.1109/EuroSP53844.2022.00032`.

Appendix A Implementation Details

A.1 Suricata Firewall Rules

Listing 1 Firewall Rules For Routing Packets To Suricata.

```
        ## Start Suricata NFQUEUE rules
        -I INPUT 1 -p tcp --dport 22 -j NFQUEUE --queue-bypass
        -I OUTPUT 1 -p tcp --sport 22 -j NFQUEUE --queue-bypass
        -I FORWARD -j NFQUEUE
        -I INPUT 2 -j NFQUEUE
        -I OUTPUT 2 -j NFQUEUE
        ## End Suricata NFQUEUE rules
```

A.2 Python Scripts

A.2.1 Fetching IoCs from MISP

Listing 2 Script to Fetch IOCs from MISP.

```
{Python}

        from pymisp import PyMISP, MISPEvent


        # Initialize misp

        misp = PyMISP(MISP_URL, MISP_API_KEY, ssl=False)

        def fetch_iocs():

            """Fetches Indicators of Compromise (IOCs)

                from a MISP instance."""

            events = misp.search(controller='events',

                                    return_format='json',

                                    published=True)

            iocs = set()

            if isinstance(events, list) and len(events) > 0:

                for event in events:

                    event_data = event.get('Event')

                    if event_data:

                        attributes = event_data.get('Attribute', [])

                        for attr in attributes:

                            if attr['type'] in

                                        ['ip-src', 'domain', 'url']:

                                iocs.add(attr['value'])

            return iocs
```

A.2.2 Generating Mitigation with AI

Listing 3 Script to Send Email Notifications.

```
{Python}

        import cohere


        def generate_mitigation_info(log):
            """Generate mitigation info by sendind
            the log entry to the LLM"""

            co = cohere.Client(cohere_api_key)
            prompt = f"Explain the following log entry and
            provide mitigation steps as to a layman:\n\n{log}"
            response = co.generate(
                model='command-xlarge-nightly',
                prompt=prompt,
            )

            return response.generations[0].text
```

A.2.3 Sending Email Notifications

Listing 4 Script to Send Email Notifications.

```
{Python}

        def send_email(subject, body):

            """Send an email with the given subject and body."""

            mail = mt.Mail(

                sender=mt.Address(email="mailtrap@demomailtrap.com",

                name="Action Required: "),

                to=[mt.Address(email=recipient)],

                subject=subject,

                text=body,

                category="Integration Test",

            )

            client = mt.MailtrapClient(token=mailtrap_token)


            response = client.send(mail)

            return response
```