Online-Journals.org

iJIM International Journal of Interactive Mobile Technologies

iJIM | eISSN: 1865-7923 | Vol. 19 No. 2 (2025) | OPEN ACCESS

https://doi.org/10.3991/ijim.v19i02.52377

PAPER

Analyzing and Mitigating Attacks in IoT Smart Home Using a Threat Modeling Approach-Based STRIDE

Mariya Ouaissa[1](✉), **Mariyam Ouaissa**[2]

[1]Computer Systems Engineering Laboratory, Cadi Ayyad University, Marrakech, Morocco

[2]Laboratory of Information Technologies, Chouaib Doukkali University, El Jadida, Morocco

m.ouaissa@uca.ac.ma

ABSTRACT

The Internet of Things (IoT) is a network of interconnected devices that enables data exchange. It is widely used in areas such as healthcare, aviation, agriculture, energy, and home automation. Despite its rapid growth and the massive adoption of connected devices, IoT presents significant security risks. Traditional threat modeling approaches are insufficient to address these risks. Architecture-based modeling is recommended, as it considers the entire system and helps in understanding potential threats. Threat modeling is a systematic technique used to identify and evaluate potential threats that could compromise the security of a system. The main objective is to understand the vulnerabilities of a system in order to design appropriate security measures to mitigate them. This paper aims to analyze and mitigate specific IoT smart home threats using the STRIDE threat modeling framework, which systematically identifies potential vulnerabilities at the development level. By applying STRIDE, which stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege, we focused on addressing key security threats, including denial of service (DoS), phishing, and man-in-the-middle (MitM) attacks. Our findings demonstrate that the proposed mitigation strategies are effective in countering these threats, providing a robust security layer for IoT smart homes. Through this study, we highlight the importance of architecture-based threat modeling to enhance security within the IoT ecosystem and offer practical solutions that strengthen IoT smart home resilience. The outcomes of the STRIDE-based analysis and the effectiveness of the mitigation techniques are detailed, offering empirical evidence to support our approach.

KEYWORDS

Internet of Things (IoT), smart home, threat modeling, STIRDE, security threats, denial of service (DDoS), man-in-the-middle (MitM), phishing, mitigation techniques

1 INTRODUCTION

In recent years, thanks to the continuous miniaturization of electronic components and technological innovations in digital communication, the number of connected smart objects has steadily increased across all application domains. A smart

Ouaissa, M., Ouaissa, M. (2025). Analyzing and Mitigating Attacks in IoT Smart Home Using a Threat Modeling Approach-Based STRIDE. *International Journal of Interactive Mobile Technologies (iJIM)*, 19(2), pp. 126–142. https://doi.org/10.3991/ijim.v19i02.52377

Article submitted 2024-09-23. Revision uploaded 2024-10-28. Final acceptance 2024-10-29.

object is a physical or virtual machine that must possess some computing and memory capacity in addition to being autonomous; that is, it can process data and sometimes even make decisions without human intervention. Furthermore, it can connect with any other object in a flexible and seamless manner. This network of connected objects, known as the Internet of Things (IoT), can assist humans in daily activities through its detection, computing, and communication capabilities [1].

The use of connected devices in perceptive environments, such as smart homes, offers new opportunities to enhance the quality of life and has direct applications in home-based assisted living. With the aging population in developed countries, smart homes are increasingly seen as a solution to help elderly individuals remain in their homes for longer periods. These homes also provide significant benefits to people with mobility issues, enabling greater autonomy and improving their comfort of life [2]. The use of self-monitoring equipment is another solution that allows for the monitoring of certain physiological parameters in dependent individuals, providing precise information about their health status to detect potential deteriorations and ensure optimal medical care.

However, the proliferation of these connected objects, which handle sensitive personal data, poses a threat to the privacy of their users. Information about habits, illnesses, and personal circumstances could be exploited by unauthorized individuals seeking illicit gain. This is why the security and confidentiality of user data are critical challenges for the IoT. Additionally, the use of the IoT introduces challenges for implementing traditional security tools. The scarcity of resources in terms of energy, memory, and computing power, which characterizes connected objects, limits the deployment of conventional security solutions [3].

Threat modeling is an effective approach to securing systems, applications, networks, and services. It employs engineering techniques to identify threats and offer recommendations for reducing risks, thus achieving security objectives earlier in the development lifecycle. In our work, the proposed methodology for threat modeling consists of six major steps. These steps include use case description (in our case, the IoT smart home), security requirements analysis, data flow and process flow diagram generation, threats identification, threat used identification (in our case DDoS, MitM, and phishing attacks), and threat mitigation (see Figure 1). Various threat modeling tools are available, but we chose STRIDE, a tool developed by Microsoft, for our modeling [4]. During the development of our model, we focused on the design at the component level to identify all potential attack vectors within and between nodes.

Our goal in this paper is to identify and mitigate potential security risks and threats to ensure the integrity and privacy of IoT smart home systems. Our model highlights significant cybersecurity threats within this system. By addressing these threats, we can develop effective countermeasures to create a robust and cyber-secure system. The structure of this paper is as follows: Section 2 provides an overview of IoT smart home background and the vulnerabilities in this system, followed by Section 3 discussing the threat modeling methodology and tools. Section 4 presents the results along with discussion. Conclusions are drawn in Section 5.

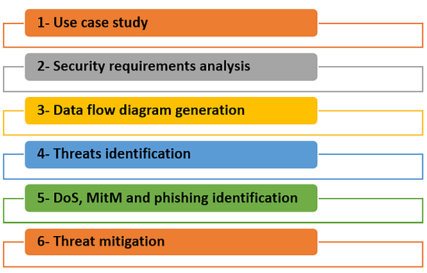

Fig. 1. Threat modeling process for IoT smart home

2 BACKGROUND

The IoT is a paradigm that has become an integral part of everyday life for every human being. IoT now encompasses a vast array of objects equipped with sensors, actuators, and communication modules that allow them to connect to the Internet. These devices observe and interact with the real world, acting as a bridge between real life and the digital world. IoT offers numerous advanced services, such as real-time automatic monitoring of industrial, medical, agricultural, and home automation environments, among others, which can be automatically managed and controlled [5]. In this section, we will discuss the concept of one of the most widespread IoT applications: the IoT smart home. We will also identify the main vulnerabilities that can affect this service.

2.1 Internet of things smart home

The concept of the smart home emerged from the convergence of new ideas in ubiquitous computing and home automation, as well as the favorable context of the home environment, which serves as a cutting-edge application area for exploring their innovative potential. Smart home technologies include sensors, actuators, devices, and peripherals that are networked to enable automation and both local and remote control of the domestic environment. Controllable devices include heating and hot water systems, lighting, windows, curtains, garage doors, refrigerators, televisions, and washing machines. As a result, beyond their usual functions, these devices can be accessed and controlled remotely. These devices act as access points offering various services. Sensors detect environmental parameters such as temperature, light, movement, and humidity. An example of smart home services is gathering information from sensors to instruct actuators to perform specific actions. For instance, in a smart home, it is common to have one or more temperature sensors that communicate with the central heating system to maintain a specific ambient temperature in the home or even in each room. In other words, these smart objects enhance existing installations by increasing comfort, thus contributing to the realization of connected homes.

The ability to control smart home systems is provided either through software installed on computing devices such as smartphones, tablets, laptops, personal computers, etc., or through dedicated hardware interfaces, such as control and command screens mounted on walls. The various devices are networked, typically using wireless technology, with the help of standardized communication protocols [6]. The diversity of devices and technologies offers great flexibility in their deployment within smart homes. The intelligence of these new homes lies in the multitude of new services they offer and how these services are organized. Home automation encompasses all the technologies of electronics, computing, and telecommunications used in homes to make them "smarter." It aims to integrate various systems that can connect to each other and to internal and external communication networks. Indeed, home automation leverages IoT techniques to connect different devices and systems within a home, allowing for remote control and automation of domestic tasks [7].

The services offered by smart homes cover three main areas:

1. **Energy management:** Regulating temperature, lighting, ventilation, and appliances to improve the home's energy efficiency.
2. **Security and surveillance:** Security systems, surveillance cameras, intrusion alarms, and other security devices to protect the home and its occupants from intrusions, fires, and other hazards.

3. **Comfort and convenience:** Remote control of devices, entertainment systems, automation of household tasks, and other features to enhance the comfort and convenience of the home.

2.2 The architecture of IoT smart home

The architecture of a surveillance and control system for a smart home consists of four main components. First, the detection part includes connected sensors and actuators, which collect data such as temperature, humidity, light levels, and presence, and control equipment like air conditioners. Next is the communication part, which uses protocols such as Wi-Fi and MQTT to exchange data between sensors and the application server. The third component is the application server, which manages the data flows captured by the sensors and stores the data in the storage system. Finally, the fourth component is the end-user interface, where the user can access the collected information, including traceability, alerts, and remote control of equipment (see Figure 2) [8].

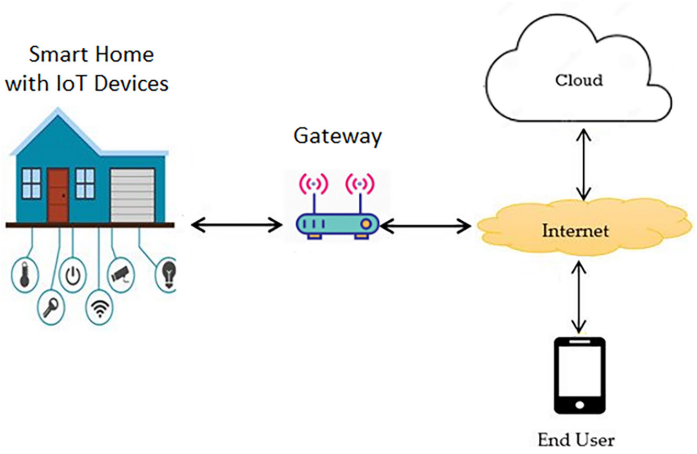

Fig. 2. IoT smart home architecture

IoT device zone: This zone includes sensors and devices that measure physical or environmental data such as temperature, humidity, motion, and light. These sensors are often installed in different parts of the home to collect environmental information. According to recent reports, the number of IoT devices in smart homes has grown significantly. For instance, the global smart home market is projected to grow from $79.5 billion in 2020 to $313.95 billion by 2026, reflecting a compound annual growth rate (CAGR) of 25%. In addition, studies estimate that there will be over 75 billion connected IoT devices by 2025, with a significant portion used in residential settings. These statistics underscore the growing importance of addressing security concerns in IoT smart homes, which is the focus of our work.

IoT field gateway zone: The IoT gateway is a device that acts as a bridge between local IoT devices and the cloud. It collects data from sensors and local devices, processes it, and sends it to the cloud for further storage or analysis. The gateway also manages communications between the different devices and systems within the home.

Cloud zone: The IoT Cloud is the remote infrastructure where data collected by sensors and devices is stored and processed. It offers scalable storage, computing capabilities, and data analysis services. The data stored in the cloud can be accessed from anywhere via an application or web interface.

2.3 Vulnerabilities associated with IoT smart home

Smart objects are often deployed in open environments where they are not constantly monitored. For example, when battery-powered sensors are deployed in the field to collect environmental data such as temperature, pressure, humidity, and light levels, they typically operate without continuous physical supervision by the operator. However, an adversary could gain physical access to these devices to carry out attacks, such as copying collected data to compromise confidentiality or altering or deleting data to undermine integrity. The nodes themselves could be cloned or modified without the owner's knowledge.

Moreover, due to the limited resources of IoT devices, communication protection mechanisms are often not implemented, which could allow an adversary to eavesdrop on communications, forge exchanges, and more. In the domain of home surveillance applications, ubiquitous devices like surveillance cameras increasingly provide information about users' daily lives, making it essential that this private information remains secure. Therefore, these devices must be secured to prevent unauthorized local and remote access, ensuring the protection of the data they produce [9].

The widespread acceptance and adoption of IoT depend on the implementation of security mechanisms to protect both the connected objects themselves and the data they send and receive. These mechanisms are the foundational building blocks for designing secure IoT solutions to collect, transmit, and store sensitive information.

Many IoT devices come with default credentials that are often not changed by users, making them vulnerable to attacks like brute force or credential stuffing. This is a significant weakness in smart home systems, where devices such as cameras or smart locks can be easily compromised if proper password policies are not enforced.

3 METHODOLOGY

Following the use case description and security requirements analysis, the next step involves creating flow diagrams for the IoT smart home use case, which will serve as the basis for identifying potential threats. In this section, we will cover the threat modeling methodology, including the threat modeling tool used, the generation of Data Flow Diagrams, and the identification of threats.

3.1 Threat modeling

Threat modeling is an effective method for securing systems, applications, networks, and services. It involves identifying potential threats and providing recommendations to reduce risks and attain security objectives earlier in the development lifecycle. A key aspect of threat modeling is the utilization of a data flow diagram, which visually illustrates how the system functions [10]. Subsequently, a framework is applied to facilitate the identification and resolution of security issues. Systems released without prior threat modeling expose both customers and organizations to significant risks. Threat modeling is a technique accessible to anyone familiar with their system's operation and possessing a basic understanding of information security. The technique is segmented into four distinct phases, each comprising crucial steps enabling the creation of a data flow diagram (DFD) and its subsequent analysis for potential threats [11]. Table 1 provides a description of each phase.

Table 1. Description of the threat modeling phases

Phase	Title	Description
1	Design	Document all your system requirements and develop a data flow diagram.
2	Detection	Utilize a threat modeling framework to analyze the data flow diagram and identify possible security vulnerabilities.
3	Correction	Determine the most suitable approach for addressing each security concern by selecting the appropriate combination of security controls.
4	Verification	Ensure that requirements are fulfilled, issues are identified, and security controls are effectively implemented.

Following the analysis of the IoT smart home system and its security requirements, the next step is to create flow diagrams for this system, which will facilitate threat identification. Various threat modeling tools are available, including threat modeler, OWASP threat dragon, and Microsoft's threat modeling (MTM) tool.

The DREAD model is a framework and approach used in threat modeling that explores a quantitative assessment of the threats' severity, impact, and occurrence. The term DREAD stands for: D – damage potential, R – reproducibility, E – exploitability, A – affected users, D – discoverability. For each stage, a rating on a scale from 1 to 10 is required to evaluate the threat impact and graveness, so the security team could know which ones should be prioritized and focused on; however, DREAD is considered a limited model since it's complicated and subjective. Dragon is a tool from OWASP dedicated to creating threat model diagrams to help security teams identify threats, indicate the most potential ones, and propose solutions to remedy them. Dragon is usually used by developers and technical profiles thanks to its simplicity, flexibility, efficiency, and accessibility.

We opted for the MTM tool due to its strong support for developing IoT use cases and its effectiveness in identifying design-level threats. Using MTM, we constructed the DFD for the specified use case. This tool is an essential part of the Microsoft security development lifecycle (SDL), enabling software architects to identify and resolve potential security vulnerabilities early in the development process, making them easier and less costly to address. As a result, it significantly reduces overall development costs. Additionally, the tool is designed with non-security experts in mind, simplifying the threat modeling process for all developers by providing expert guidance on creating and analyzing threat models. Typically, Microsoft employs the STRIDE framework, which categorizes threats into six major categories: 1) spoofing, 2) tampering, 3) repudiation, 4) information disclosure, 5) denial of service (DoS), and 6) elevation of privilege. This categorization aids in formulating specific questions and streamlining security discussions, providing a comprehensive, though not exhaustive, overview of potential threats [12].

Spoofing: This refers to the unauthorized acquisition and use of another user's authentication credentials, including usernames and passwords. For example, in a smart home environment, an attacker could spoof a smart lock's credentials, gaining unauthorized access to the home by posing as the homeowner.

Tampering: This involves the malicious modification of data. Examples include unauthorized changes to persistent data stored in databases and the manipulation of data being transmitted between two computers over an open network, such as the Internet.

Repudiation: This pertains to users denying their actions without the ability for others to prove otherwise. For instance, if a user performs an illicit operation within a system that lacks the capability to track such actions, they can disavow their involvement. Non-repudiation refers to a system's ability to counter these

repudiation threats. For example, when a user makes a purchase, they may be required to provide a signature upon receipt of the item. The supplier can then use this signed acknowledgment of receipt as evidence of the delivery to the user.

Information disclosure: This involves the unauthorized exposure of information to individuals who should not have access. Examples include instances where users can access files they are not permitted to view or where intruders intercept data being transmitted between two computers.

Denial of service: DoS attacks prevent legitimate users from accessing services, such as making a web server temporarily unavailable or unusable. It is crucial to protect against specific types of DoS threats to enhance system reliability and availability. For example, an attacker could flood the smart home network, preventing homeowners from controlling their smart devices remotely or even disabling essential systems such as alarms or cameras.

Elevation of privilege: This occurs when a user with insufficient privileges gains access to privileged accounts, allowing them to compromise or dismantle the entire system. Elevation of privilege threats include scenarios where an attacker bypasses all system defenses and integrates into the trusted system, creating a highly dangerous situation. In a smart home, an attacker might exploit a vulnerability in the smart hub or central controller, gaining administrative control over the entire smart home system. This would allow them to manipulate devices, deactivate alarms, or access private data, potentially compromising the entire smart home network.

3.2 Data flow diagram generation

Figure 2 depicts the DFD for the IoT smart home system, created using the Threat Modeling tool. The diagram is based on the IoT smart home system architecture and security requirements discussed earlier [13]. In Figure 3, rectangular shapes with solid black borders represent IoT devices and databases, such as azure storage, while circular shapes denote data processing components like azure stream analytics, data virtualization, and presentation. Green rectangles indicate the transmission of requests and responses between components. Each zone is outlined with red dotted lines. Consistent with the design hierarchy described previously, the IoT devices are positioned on the left side of Figure 3, connected to the IoT field gateway. The IoT field gateway is further linked to the cloud zone, which includes two sub-zones: the IoT cloud gateway zone and the Azure zone. Users in the consumer zone can send requests to the Azure server, with data flowing from the cloud zone to the IoT device zone via the IoT cloud gateway.

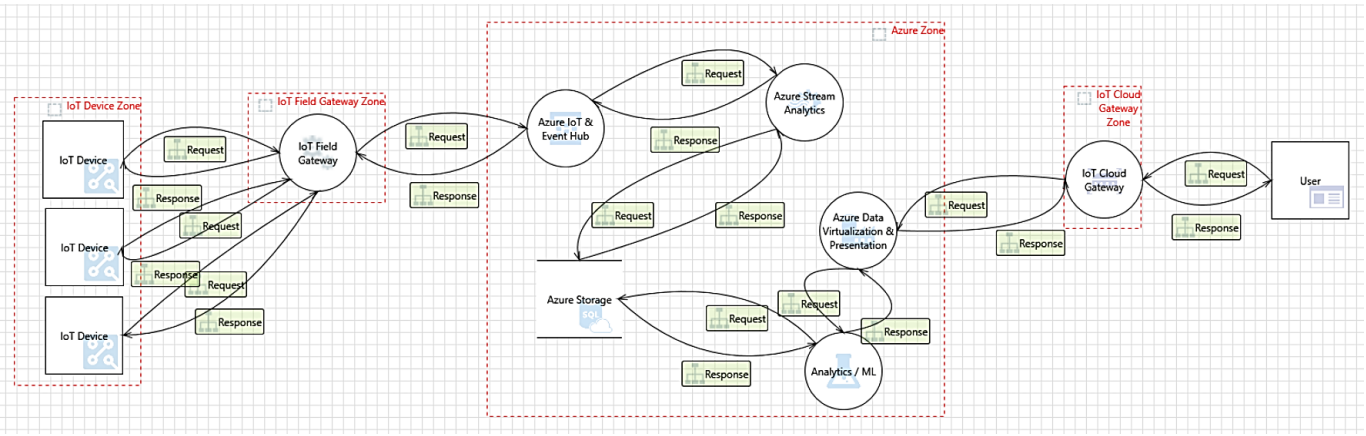

Fig. 3. Data flow diagram in MTM tool

3.3 Threats identification

Following the application of the threat modeling approach, the next step is threat identification, as illustrated in Figure 3. By employing the STRIDE threat modeling technique within the MTM tool, a detailed threat report was generated for each component in the DFD. Subsequently, all identified threats were documented separately in Section 4 of the results. These listed threats highlight how specific components can be compromised by various threats. We also detailed the assets impacted by each STRIDE threat and their correlation with security requirement violations. After cataloging all the threats identified through the STRIDE technique, we further analyzed which of these threats could lead to DoS, phishing and man-in-the-middle (MitM) attacks.

3.4 Denial of service threat identification

In a smart home environment, many IoT devices rely on constant communication with each other, the home gateway, and the cloud to function properly. Notifications are often sent to users via mobile devices to alert them of critical events, such as security breaches, fire alarms, or abnormal sensor readings. However, these functionalities can be severely compromised by DoS attacks. In a DoS attack, an attacker floods the smart home network with excessive traffic, causing legitimate communications to fail. This can lead to the entire smart home network being overwhelmed, making it impossible for the system to relay important alerts to the user. In more targeted attacks, the adversary may focus on specific IoT devices, overloading them with traffic and rendering them nonfunctional. Such targeted DoS attacks are dangerous because they can selectively disable only certain devices, leaving other systems intact, thus going unnoticed for longer periods. The consequences of DoS attacks in smart homes range from inconvenience to critical security breaches, as a disabled device may prevent timely responses to emergencies. Mitigation strategies for DoS in smart homes include implementing rate-limiting on the network to prevent overloading and setting up robust monitoring systems to detect anomalies in network traffic, enabling early identification of DoS patterns [14].

3.5 Phishing threat identification

Phishing attacks in the context of IoT-enabled smart homes are particularly concerning because of the increasing interconnectivity between devices. In a typical phishing scenario, cybercriminals use social engineering techniques to deceive users into divulging sensitive information or granting access to smart home systems, often via fake email links, messages, or fraudulent notifications that appear legitimate. One significant risk of phishing in smart homes involves gaining unauthorized access to cloud-based platforms associated with IoT devices. Once an attacker controls these platforms, they can manipulate data streams between the cloud and devices, potentially injecting malicious commands or compromising the integrity of firmware updates. Unencrypted or improperly secured communication channels can further expose smart homes to phishing attacks, as attackers can intercept sensitive information, including login credentials or control signals. The damage from phishing can be severe attackers may take full control of smart devices, monitor

user behaviors, or even disable critical security functions. A compromised IoT system can also be leveraged for further attacks, such as integrating the devices into a larger botnet used for launching DDoS attacks against other targets. Prevention strategies include implementing strong, multi-factor authentication (MFA) for accessing IoT systems, encrypting all communications between devices and cloud services, and educating users on identifying phishing attempts [15].

3.6 Man-in-the-middle threat identification

Man-in-the-middle attacks pose a substantial threat to smart home environments due to the high volume of communication between IoT devices, gateways, and cloud services. In such attacks, a malicious actor positions themselves between two communicating parties, intercepting and potentially altering the data being transmitted. MitM attacks are particularly dangerous in smart homes because they can lead to unauthorized control of devices. For example, an attacker could intercept commands between the smart home's cloud server and a thermostat, causing temperature fluctuations without the user's knowledge. More serious consequences involve tampering with security devices such as cameras or locks, compromising the safety of the household. Additionally, sensitive information, such as user data, passwords, or device settings, can be leaked, leading to further privacy violations. Detecting MitM attacks is difficult because the malicious actor is often hidden within the network flow. However, smart homes can implement countermeasures such as strong encryption and mutual authentication protocols to ensure that only trusted devices and cloud services can communicate with each other. Network anomaly detection systems can also help identify unusual traffic patterns indicative of MitM activities, such as unexpected latency or repeated handshake failures between devices [16].

3.7 Threats mitigation

After identifying DoS, phishing, and MitM threats in the IoT smart home, the next step is to propose appropriate mitigation techniques. Threat mitigation involves reducing or eliminating potential risks within a system. To develop effective mitigation strategies, we analyzed various existing approaches and, based on these studies, selected the most suitable remedies to protect the IoT smart home use case from these potential threats, as discussed in Sections 4 and 5.

4 RESULTS AND DISCUSSION

In this section, we conduct experiments using the MTM tool to identify threats through the STRIDE methodology. In the IoT smart home system, we defined five distinct zones. We begin by identifying threats for each zone and then analyzing the identified threats that could lead to DoS, phishing, and MitM attacks. As previously discussed, STRIDE categorizes and maps the identified threats based on the use case. To achieve thorough threat identification, we integrated findings from both STRIDE methodologies to more effectively evaluate all potential threats in our IoT smart home use case. Subsequently, we propose mitigation techniques to enhance the security of the smart home against these possible attacks.

4.1 Threats identification

The IoT smart home system comprises various interconnected devices, such as smart locks, cameras, and sensors, which communicate with a central hub and a cloud-based backend. Our objective is to identify and mitigate potential security risks to ensure the integrity and privacy of the system. In this section, we examine the threats identified by the MTM tool across different zones of the IoT smart home environment.

Spoofing threats: We identified a total of 15 spoofing threats, primarily occurring in the IoT device zone and field gateways. These threats can be exploited by an attacker who reuses authentication tokens from one device on another. For instance, an attacker might extract cryptographic key material at the software or hardware level, enabling them to access the system using a different device while impersonating the original. Additionally, if multiple devices share the same Shared Access Signature (SAS) token, an attacker can spoof any device linked to that token. The lack of proper auditing and access restrictions leaves the IoT field gateway and cloud gateway vulnerable; an adversary could exploit default login credentials to access the field gateway and spoof a registered device, even if it is recognized in the cloud gateway.

Tampering threats: A total of 28 tampering threats were identified, mostly in the IoT device zone and IoT field gateway zone. In the IoT device zone, tampering threats may involve an attacker launching offline attacks by disabling the operating system or physically detaching storage media to manipulate data independently. Exploiting known vulnerabilities, particularly in outdated firmware, is also a concern. In the IoT field gateway zone, an adversary could introduce malicious code or replace the software running on the gateway, allowing the compromised software to use the device's legitimate identity if key materials are accessible. For example, an attacker might intercept and alter data in transit by leveraging stolen key material. Unauthorized access to the IoT field gateway could also allow tampering with its operating system and exposure of confidential information.

Repudiation threats: We identified 8 repudiation threats, mainly in the IoT field gateway zone and Azure zone. An adversary could engage in activities such as spoofing or unauthorized access on the field gateway, necessitating monitoring to prevent denial of involvement. Insufficient auditing may allow an adversary to deny actions performed on Azure Storage, complicating accountability.

Information disclosure threats: The MTM tool identified 11 threats related to information disclosure, primarily in the IoT device zone and Azure zone. An attacker could eavesdrop on communications between devices and the field gateway, potentially tampering with the transmitted data. If an adversary gains access to Azure virtual machines (VMs), sensitive data could be exposed if the operating system is not encrypted. Additionally, weak connection string configurations may allow unauthorized access to confidential information.

Denial of service threats: We identified 13 DoS threats affecting nearly all zones of the IoT smart home system. An attacker could overwhelm the system with malformed packets, disrupting service availability. They may also target application programming interfaces (APIs) to block access to the system.

Elevation of privilege threats: A total of 35 elevation of privilege threats were identified, with most occurring in the IoT device zone, Azure zone, IoT field gateway, and IoT cloud gateway. In the IoT device zone, an attacker could gain access to admin interfaces or privileged services, exploiting unused features or services to increase the attack surface. Insufficient authorization checks could allow unauthorized

commands to be executed remotely. Similarly, in the IoT field gateway, an adversary might exploit these checks to gain control. Unauthorized access to the IoT cloud gateway could occur if the connection is insecure. In the Azure zone, attackers could exploit unused features on Azure IoT and Event Hub, bypassing insufficient authorization checks to manage configurations or listen to events. If a device has a token with direct access to the Event Hub, it could send messages without restrictions. Additionally, weak Azure Storage configurations might allow persistent access to an Azure SQL database through compromised local user account passwords, and poorly configured account policies could enable brute force attacks on Azure Storage.

4.2 Denial of service in IoT smart home

In IoT smart home environments, DoS threats can manifest across various zones, including IoT devices, field gateways, cloud gateways, and the Azure cloud. These threats, if left unaddressed, can lead to severe consequences such as botnet attacks, DoS attacks, and unauthorized access to sensitive information.

In the IoT device zone, attackers can exploit vulnerabilities to sniff traffic from field gateways and gain unauthorized access to admin interfaces or privileges. Malicious applications or code can then be executed on compromised devices, turning them into part of a botnet under the attacker's remote control.

Similarly, in the field gateway zone, attackers may utilize jailbreaking techniques to compromise mobile devices and embed or replace malicious code, enabling remote control of user activities with root access.

The cloud gateway and Azure cloud zones are also susceptible to DoS threats. Attackers can install malicious applications or execute malicious code on devices, which can then be remotely controlled via a botmaster. This allows the attacker to monitor sensitive information and execute unwanted commands.

4.3 Phishing in IoT smart home

In IoT smart home environments, phishing threats pose significant risks across various zones, including IoT devices, field gateways, cloud gateways, and the Azure cloud. These attacks can lead to unauthorized access to sensitive information and the compromise of user privacy.

In the IoT device zone, attackers may exploit vulnerabilities to gain access to admin interfaces by sending deceptive emails or messages that appear legitimate. For example, they could impersonate device manufacturers or service providers, prompting users to click on malicious links or enter credentials on fake login pages. Once attackers obtain this information, they can take control of IoT devices, monitor user activities, and manipulate device settings.

Similarly, in the field gateway zone, phishing attacks can target mobile devices connected to the IoT smart home network. By utilizing techniques such as SMS phishing (smishing), attackers can send fraudulent messages that trick users into downloading malicious applications or revealing sensitive information, such as passwords or authentication tokens. This can lead to unauthorized access to the entire IoT smart home ecosystem.

In the cloud gateway and Azure cloud zones, phishing threats can escalate further. Attackers may send phishing emails that appear to come from cloud service providers, encouraging users to verify their accounts or update their billing information.

If users fall for these scams, attackers can gain access to cloud-based services, potentially leading to data breaches and the manipulation of stored information.

4.4 Man-in-the-middle in IoT smart home

In IoT smart home environments, MitM attacks pose significant risks across various zones, including IoT devices, field gateways, cloud gateways, and the Azure cloud. These attacks involve an attacker intercepting and potentially modifying the communication between two systems, compromising the integrity and confidentiality of the exchanged data.

For example, in the IoT device zone, an attacker could breach the communication between an IoT smart home device and the field gateway, spoofing sensor data or injecting malicious commands. This could lead to false temperature readings being sent to the cloud or the attacker disabling vulnerable HVAC systems during extreme weather conditions, causing significant disruption.

Similarly, in the field gateway and cloud gateway zones, MitM attacks can target the communication between the user's mobile device and the IoT smart home system, allowing the attacker to monitor and manipulate user interactions. This could result in the theft of sensitive data, such as personal information gathered from unprotected wearables and smart appliances, which could be exploited for identity theft or fraudulent activities.

Furthermore, in the cloud and Azure zones, MitM attacks can compromise the communication between the IoT smart home system and the cloud services, enabling the attacker to hijack devices and gain remote control over the entire IoT smart home environment. This could allow the attacker to unlock doors, change keypad PINs, or execute other malicious actions without being detected, as the attacker does not change the basic functionality of the compromised devices.

4.5 Threat mitigation techniques

Threat mitigation involves implementing strategies to reduce potential risks within a system. This process includes examining various mitigation approaches found in existing studies [17–22]. After analyzing these methods, we adopt the most effective remedies to safeguard the IoT smart home from potential threats, including DoS, phishing, and MitM attacks.

DoS threat mitigation techniques. To mitigate these risks, it is crucial to identify and properly manage DoS threats across all zones of the IoT smart home environment. Early detection and implementation of robust security measures can significantly reduce the likelihood of successful botnet attacks, DoS attacks, and unauthorized access to sensitive data. Based on the identified threats in the IoT smart home environment, several mitigation techniques are crucial for defending against DoS attacks across all zones.

Network segmentation: In an IoT smart home, network segmentation involves dividing the network into isolated sections, such as separating security devices from less critical devices. This can be achieved using VLANs or subnets, which isolate communication and contain attacks to a specific segment. For instance, a DoS attack on smart lighting won't affect security systems if they are in a separate segment. Moreover, this segmentation limits the lateral movement of attackers across the network. To implement network segmentation effectively, software-defined networking (SDN) techniques can be used to dynamically allocate bandwidth and

resources across segments based on real-time monitoring of traffic. This allows for better control and rapid response in case an attack is detected.

Traffic filtering and firewalls: At the gateway level, traffic filtering ensures that malicious or suspicious traffic is blocked before reaching IoT devices. In a smart home, firewalls can be configured to analyze traffic patterns and block unauthorized requests, while intrusion prevention systems (IPS) add another layer of defense by inspecting traffic in real time for known attack signatures. For smart homes, adaptive firewalls could be employed, which automatically adjust rules based on real-time threat intelligence. This approach ensures that firewalls can update to block new forms of DoS attacks as they evolve.

Rate limiting and device-specific controls: Rate limiting is crucial in preventing DoS attacks from overwhelming a smart home's infrastructure. In this context, rate limiting could be applied at the device and gateway levels to control the number of requests handled per second. For example, by limiting the number of requests a device can process from any single IP address, the smart home can prevent excessive traffic from causing device failure. Device-specific rate limiting can be combined with adaptive algorithms that detect abnormal spikes in traffic and automatically adjust limits. For instance, if a smart thermostat experiences a sudden, unexplained surge in traffic, the rate-limiting protocol would throttle the connections, protecting the device from being overwhelmed.

Anomaly detection with machine learning: Incorporating anomaly detection systems is essential to identify abnormal behavior indicative of a DoS attack. In smart homes, anomaly detection can be powered by machine learning algorithms that continuously learn the normal behavior patterns of IoT devices, enabling more accurate identification of unusual traffic or device behavior. For instance, if a security camera typically sends small data packets to the cloud but suddenly begins transmitting large amounts of data, anomaly detection systems would flag this as suspicious. These systems could either alert the user or automatically trigger defensive actions like isolating the compromised device.

Phishing threat mitigation techniques. To mitigate phishing threats in IoT smart home environments, it is essential to implement robust security measures. Users should be educated about recognizing phishing attempts, such as suspicious links or unexpected requests for personal information. Additionally, enabling MFA across all devices and services can provide an extra layer of security, significantly reducing the risk of unauthorized access resulting from phishing attacks. Regularly updating software and firmware for all devices can also help close vulnerabilities that attackers might exploit. In addressing phishing threats within an IoT smart home environment, several mitigation techniques are essential for protecting against attacks across all zones.

Email and message filtering: In the context of an IoT smart home, email and message filtering is critical, especially when users receive messages that might pertain to device updates, troubleshooting, or security warnings. Many phishing attempts come through emails or text messages disguised as legitimate communications from IoT device manufacturers or service providers. To mitigate this, advanced spam filters should be configured to analyze incoming messages for known phishing indicators, such as misleading links, suspicious attachments, or fake domain names. AI-based filtering tools can also be deployed to detect new and sophisticated phishing patterns, constantly evolving to recognize emerging threats that traditional filters might miss.

Multi-factor authentication (MFA): MFA is a key defense against phishing attacks that target login credentials. In a smart home environment, where multiple

devices connect to cloud services or control apps, using only a password as the single layer of defense is risky. MFA ensures that even if an attacker successfully steals a user's password through a phishing attempt, they would still need a second form of authentication, such as:

- A time-based one-time password (TOTP) generated by an authenticator application when accessing the smart home control panel.
- Biometric verification, such as fingerprint or facial recognition, which provides an additional layer of security that is difficult for attackers to bypass.

For IoT devices, especially those that do not support MFA natively, it is important to utilize an IoT gateway or central control system that enforces MFA for all devices connected to the network.

User education and training: In an IoT smart home, users themselves can often be the weakest link, as they may unknowingly fall victim to phishing attempts. Regular user education sessions could be delivered via the smart home system or application, providing practical tips on identifying phishing attempts. These could include examples of typical phishing emails or messages and instructions on how to check for common red flags. Implementing simulated phishing tests can be a proactive way to help users recognize phishing tactics in a real-world scenario. By sending fake phishing attempts to users, smart home administrators or service providers can gauge how well users are able to identify such threats and take corrective action through training if necessary.

Regular software updates: Regular updates to device firmware and software are essential to patch vulnerabilities that could be exploited by phishing attacks. For example, a smart thermostat or camera with outdated firmware might have known vulnerabilities that could allow attackers to gain unauthorized access through phishing attacks aimed at exploiting those weaknesses. Automated update mechanisms should be enabled where possible to ensure devices stay up-to-date without requiring user intervention. This reduces the chances of devices running outdated software that might be vulnerable. Users should be notified when updates are available and instructed on how to apply them if automation is not feasible, ensuring that they are always running the latest and most secure version of the software.

Man-in-the-middle threat mitigation techniques. To mitigate these risks, it is crucial to implement robust security measures, such as secure boot, mutual authentication between devices and services, and end-to-end encryption of data. By ensuring the integrity and confidentiality of communication across all zones, the impact of MitM attacks can be significantly reduced, safeguarding the privacy and security of IoT smart home environments.

To mitigate MitM attacks within an IoT smart home environment, several key strategies should be implemented across all zones.

End-to-end encryption (E2EE): E2EE is a fundamental defense against MitM attacks because it ensures that data exchanged between IoT devices, gateways, and cloud services is encrypted and can only be decrypted by the intended recipient. Even if a MitM attacker intercepts the data, they won't be able to decipher it. TLS should be used for encrypting communications between devices and cloud services. In IoT environments, this may also include securing device-to-device communications within the local network. Implementing perfect forward secrecy (PFS) within the encryption protocols can further strengthen the security, ensuring that even if long-term keys are compromised, previous communications remain secure.

Strong authentication mechanisms: Mutual authentication between IoT devices and cloud services is essential to prevent unauthorized access and MitM attacks. This ensures that both the device and the cloud service verify each other's identity before establishing a connection. Using MFA adds an extra layer of security by requiring an additional form of verification when accessing the smart home system or its devices. Secure key exchange protocols, such as Diffie-Hellman or elliptic curve cryptography (ECC), should be used during device onboarding to securely exchange encryption keys and authenticate devices, reducing the risk of MitM attacks during the initial connection setup.

Regular security audits and vulnerability assessments: Conducting regular security audits ensures that potential weaknesses in the network or devices are identified and remediated before they can be exploited by attackers. These audits should involve reviewing encryption configurations, access control settings, and firewall rules. Penetration testing should be performed periodically to simulate attack scenarios, helping to identify potential vulnerabilities that could be exploited in MitM attacks. Vulnerability scanning tools should be employed to continuously monitor the network for known vulnerabilities in devices and gateways, ensuring that patches and updates are applied promptly.

Secure device provisioning: During the initial setup of an IoT device, secure provisioning ensures that only trusted devices are authenticated and allowed to join the smart home network. This is especially important for devices that connect to cloud services or critical parts of the smart home system. Device manufacturers should implement unique cryptographic keys and certificates for each device, ensuring secure onboarding processes that prevent rogue devices from gaining access to the network. PKI (Public Key Infrastructure) can be used to manage device certificates, ensuring that only authorized devices are trusted within the IoT ecosystem.

Intrusion detection systems (IDS): IDS can monitor network traffic for signs of MitM attacks, such as unusual traffic patterns, delays in communications, or mismatched data transmissions. In a smart home, IDS tools can be deployed at both the local network and gateway levels to detect and respond to threats. Advanced IDS solutions can integrate machine learning algorithms to detect anomalies in device behavior, providing early warnings of potential MitM attacks by identifying deviations from normal traffic flows or communication patterns. Alert mechanisms should be set up to notify users or system administrators when suspicious activities are detected, allowing for quick mitigation actions, such as isolating affected devices or segments.

5 CONCLUSION

The widespread adoption of IoT devices in IoT smart home environments has introduced significant security risks that must be addressed proactively through comprehensive threat modeling. This paper presents a methodology that leverages the STRIDE framework to systematically analyze potential threats within an IoT smart home scenario, focusing on key attack vectors such as DoS, phishing, and MitM. By identifying development-level threats specific to the IoT smart home context and correlating them with appropriate mitigation strategies, the proposed approach enhances the overall security posture of IoT systems. As IoT continues to evolve, proactive and comprehensive threat modeling will be crucial in safeguarding against emerging security risks and ensuring the resilience of IoT smart home environments. This work can be further enhanced by implementing the proposed

mitigation techniques in a real-world system, allowing for deeper insights into securing the underlying infrastructure against DoS, phishing, and MitM attacks.

6 REFERENCES

[1] M. Ouaissa, A. Rhattoy, and I. Chana, "New security level of authentication and key agreement protocol for the IoT on LTE mobile networks," in *Proceedings of 2018 6th International Conference on Wireless Networks and Mobile Communications (WINCOM)*, 2018, pp. 1–6. https://doi.org/10.1109/WINCOM.2018.8629767

[2] A. Chakraborty, M. Islam, F. Shahriyar, S. Islam, H. U. Zaman, and M. Hasan, "Smart home system: A comprehensive review," *Journal of Electrical and Computer Engineering*, vol. 2023, no. 1, p. 7616683, 2023. https://doi.org/10.1155/2023/7616683

[3] M. Ouaissa and M. Ouaissa, "Cyber security issues for IoT based smart grid infrastructure," in *IOP Conference Series: Materials Science and Engineering*, IOP Publishing, vol. 937, 2020, p. 012001. https://doi.org/10.1088/1757-899X/937/1/012001

[4] A. Konev, A. Shelupanov, M. Kataev, V. Ageeva, and A. Nabieva, "A survey on threat-modeling techniques: Protected objects and classification of threats," *Symmetry*, vol. 14, no. 3, p. 549, 2022. https://doi.org/10.3390/sym14030549

[5] M. Ouaissa, M. Ouaissa, and A. Rhattoy, "An efficient and secure authentication and key agreement protocol of LTE mobile network for an IoT system," *Int. J. Intell. Eng. Syst.*, vol. 12, no. 4, pp. 212–222, 2019. https://doi.org/10.22266/ijies2019.0831.20

[6] G. Vardakis, G. Hatzivasilis, E. Koutsaki, and N. Papadakis, "Review of smart-home security using the Internet of Things," *Electronics*, vol. 13, no. 16, p. 3343, 2024. https://doi.org/10.3390/electronics13163343

[7] V. A. Orfanos, S. D. Kaminaris, P. Papageorgas, D. Piromalis, and D. Kandris, "A comprehensive review of IoT networking technologies for smart home automation applications," *Journal of Sensor and Actuator Networks*, vol. 12, no. 2, p. 30, 2023. https://doi.org/10.3390/jsan12020030

[8] O. Djumanazarov, A. Väänänen, K. Haataja, and P. Toivanen, "An overview of IoT-based architecture model for smart home systems," in *Proceedings of International Conference on Intelligent Systems Design and Applications*, Cham: Springer International Publishing, 2021, pp. 696–706. https://doi.org/10.1007/978-3-030-96308-8_65

[9] S. Uppuluri and G. Lakshmeeswari, "Review of security and privacy-based IoT smart home access control devices," *Wireless Personal Communications*, vol. 137, pp. 1601–1640, 2024. https://doi.org/10.1007/s11277-024-11405-8

[10] W. Xiong and R. Lagerström, "Threat modeling–A systematic literature review," *Computers & Security*, vol. 84, pp. 53–69, 2019. https://doi.org/10.1016/j.cose.2019.03.010

[11] S. Hussain, A. Kamal, S. Ahmad, G. Rasool, and S. Iqbal, "Threat modelling methodologies: A survey," *Sci. Int. (Lahore)*, vol. 26, no. 4, pp. 1607–1609, 2014.

[12] A. Seeam, O. S. Ogbeh, S. Guness, and X. Bellekens, "Threat modeling and security issues for the Internet of Things," in *Proceedings of 2019 Conference on Next Generation Computing Applications (NextComp)*, 2019, pp. 1–8. https://doi.org/10.1109/NEXTCOMP.2019.8883642

[13] A. R. Mahlous, "Threat model and risk management for a smart home IoT system," *Informatica*, vol. 47, no. 1, pp. 52–64, 2023. https://doi.org/10.31449/inf.v47i1.4526

[14] M. Tehaam, S. Ahmad, H. Shahid, M. S. Saboor, A. Aziz, and K. Munir, "A review of DDoS attack detection and prevention mechanisms in clouds," in *Proceedings of 2022 24th International Multitopic Conference (INMIC)*, 2022, pp. 1–6. https://doi.org/10.1109/INMIC56986.2022.9972962

[15] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, "Phishing attacks: A recent comprehensive study and a new anatomy," *Frontiers in Computer Science*, vol. 3, p. 563060, 2021. https://doi.org/10.3389/fcomp.2021.563060

[16] M. Thankappan, H. Rifà-Pous, and C. Garrigues, "Multi-channel man-in-the-middle attacks against protected Wi-Fi networks: A state-of-the-art review," *Expert Systems with Applications*, vol. 210, p. 118401, 2022. https://doi.org/10.1016/j.eswa.2022.118401

[17] B. Prabadevi and N. Jeyanthi, "A review on various sniffing attacks and its mitigation techniques," *Indones. J. Electr. Eng. Comput. Sci*, vol. 12, no. 3, pp. 1117–1125, 2018. https://doi.org/10.11591/ijeecs.v12.i3.pp1117-1125

[18] B. Naqvi, K. Perova, A. Farooq, I. Makhdoom, S. Oyedeji, and J. Porras, "Mitigation strategies against the phishing attacks: A systematic literature review," *Computers & Security*, vol. 132, p. 103387, 2023. https://doi.org/10.1016/j.cose.2023.103387

[19] A. K. Jain and B. B. Gupta, "A survey of phishing attack techniques, defence mechanisms and open research challenges," *Enterprise Information Systems*, vol. 16, no. 4, pp. 527–565, 2022. https://doi.org/10.1080/17517575.2021.1896786

[20] M. F. Alghenaim, N. A. A. Bakar, F. Abdul Rahim, V. Z. Vanduhe, and G. Alkawsi, "Phishing attack types and mitigation: A survey," in *Proceedings of the International Conference on Data Science and Emerging Technologies*, Singapore: Springer Nature Singapore, vol. 165, 2022, pp. 131–153. https://doi.org/10.1007/978-981-99-0741-0_10

[21] O. Salem, K. Alsubhi, A. Shaafi, M. Gheryani, A. Mehaoua, and R. Boutaba, " Man-in-the-Middle attack mitigation in Internet of Medical Things," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 3, pp. 2053–2062, 2021. https://doi.org/10.1109/TII.2021.3089462

[22] L. Daoud and N. Rafla, "Efficient mitigation technique for Black Hole router attack in Network-on-Chip," *Microprocessors and Microsystems*, vol. 94, p. 104658, 2022. https://doi.org/10.1016/j.micpro.2022.104658

7 AUTHORS

Mariya Ouaissa is a Professor in Cybersecurity and Networks at FSSM, Cadi Ayyad University, Marrakech, Morocco. She is a Ph.D., graduated in 2019 in Computer Science and Network from ENSAM, Moulay Ismail University, Meknes, Morocco. Her main research topics are Cybersecurity, IoT, M2M, D2D, WSN, Cellular Networks, Vehicular Networks. She has published over than 70 papers (Book Chapters, International Journals, and Conferences/Workshops), 20 Edited Books, and 10 Special Issues as guest editor (E-mail: m.ouaissa@uca.ac.ma).

Mariyam Ouaissa is currently an Asssitant Professor in Netwroks and Systems at ENSA, Chouaib Doukkali University El Jadida, Morocco. She is a Ph.D. in Computer Science and Networks graduated in 2019 from Moulay Ismail University, ENSAM, Meknes, Morocco. Her main research topics are IoT, M2M, WSN, Vehicular Networks, Cellular Networks. She is mainly working on M2M congestion overload problem, security and the resource allocation management. She has published more than 60 research papers. She is Editor for some of the popular books published by the likes of Springer, De Gruyter, RGN Publications, etc. and Guest Editor in several special issues of reputed journals.