Security and Privacy in Internet of Things: Attacks and Best Practices in the Smart Home Scenario

Sassi Gabriele

Abstract
IoT systems are characterized by numerous and different devices that handle vast amounts of sensitive information. The heterogeneity and limited computational resources introduce significant vulnerabilities, necessitating ad-hoc solution which respect to traditional security measures.
The aim of this paper is to provide a comprehensive overview of current IoT security requirements, potential vulnerabilities, and types of attacks, particularly focusing on smart homes. This study clearly demonstrates that while numerous best practices and solutions for enhancing IoT security and privacy exists, with significant advancements in security protocols, encryption methods, and intrusion detection systems; there is no single, unified, and well-defined approach that comprehensively addresses cyber, physical and human aspects.

1. Introduction

An IoT system, from a logical perspective, can be described as a network of intelligence devices working together to achieve a shared goal. At the technical level, IoT implementations can adopt a variety of processing and communication structures, technologies and designed approach to satisfy particular purposes, such as acquiring data of interest in a certain scenario [1].
Consequently, a global network infrastructure is emerging, supporting systems that include an extremely large number of heterogeneous devices, including sensors, actuators, RFID, NFC, supporting the provisioning of innovative and customized services to individuals in different application domains.
The high level of diversity between communication protocols and standards, the computation, energy and bandwidth constraints, the big amount of sensitive information handled (e.g, user habits) and the expansive scale of IoT systems expose the network vulnerable to a range of attacks targeting resources (e.g, DoS attack), integrity and confidentiality of transmitted data (e.g., man-in-the-middle, packet sniffing), source authentication (e.g. compromised keys, session violation) and the privacy of users leveraging IoT services [2] .

Traditional security measures and privacy enforcement cannot be directly applied to IoT technologies due to their hardware and software limitation. However, it is essential to ensure confidentiality and integrity alongside authentication and authorization mechanisms to prevent unauthorized access. Concerning privacy, both data protection and anonymization of users' personal information must be safeguarded with flexibility, considering user needs and rights. The primary objective of this paper is to analyze the security issues and attacks related to a smart home scenario, by firstly providing, in Section 2, a comprehensive overview of the current state-of-the-art in IoT security requirements and vulnerabilities focusing on smart home cybersecurity, followed by Section 3 which provides a detailed examination of vulnerabilities and potential attacks within the scenario.
The suggested solutions and best practices are provided in Section 4. Finally, Section 5 concludes this paper.

2. Related works

In IoT environments it's essential to focus, with a deep analysis on three two key security requirements. IoT, enables a constant transfer and sharing of data among things and users to achieve a particular goal. Authentication, authorization, access control and non-repudiation are important to ensure secure communication. However, the lack of computing resources requires to taylor existing techniques to this new environment. As regard authentication, the authors in [3] introduce the first fully implemented two-way authentication security scheme for IoT, which leverages existing internet standards, specifically the Datagram Transport Layer Security (DTLS) protocol. This protocol operates between the transport and application layers. The scheme utilizes RSA encryption and is designed for IPv6 over 6LoWPANs. Another authentication protocol for IoT is presented in [4], using lightweight encryption method based on XOR manipulation. The authentication and access control method presented in [5] aims at establishing the session key based on Elliptic Curve Cryptography (ECC), by defining attributed based access control policies, enhancing mutual authentication among user and sensor nodes. As regard confidentiality and integrity, a pratical approach in [6], proposes a transmission model with signature-encryption schemas, which addresses IoT security requirements, especially in attack-resistance, by means of Object Naming Service queries. Despite that, a unique and well-defined solution able to guarantee confidentiality in IoT context is still missing, also asserted in [7]. Finally, for all scenarios, users require the protection of their personal information related to their movements, habits and interactions with other devices and people. Privacy must be guaranteed. Despite using different approaches, [8], [9], [10] all employs the same privacy-preserving technique known as k-anonymity, ensuring sensitive data privacy by creating k-anonymized clusters that protect quasi-identifier attributes of data tuples. Researchers and experts are constantly exploring new approaches to secure IoT devices, which are continuously exposed, due to vulnerabilities posed by their unique constraints, to different threats. In the case of a smart home scenario, an attacker might attempt to fabricate, intercept, manipulate, or interrupt the transmitted data. The research in [11] divided the threats of cyberattacks in two categories. Target and non-targeted attacks. The first ones infect victims randomly without specific selection criteria, aiming to compromise as many systems as possible for monetary gains from selling or exploiting extracted information. In contrast, targeted attacks usually exhibit a higher degree of sophistication, with attackers specifically selecting victims believed to possess valuable information. Furthermore, the research in [12] discusses two types of attacks on smart home systems: internal and external entity attacks. These attacks can be executed passively or actively, depending on the attackers' objectives. Passive attackers focus on communications to gather significant information, which can be used to observe user behavior or store for future active attacks. In contrast, active attackers aim to compromise users' privacy, security, and confidentiality, as well as impact data integrity, gain unauthorized access, and disrupt the smart home functions that provide essential services. Both types of attacks target the smart home's infrastructure and the information stored in cloud services. Moreover, [13] classified various types of cybercriminals along their objectives. This classification provides a better understanding of the types of intruders, their goals, what they aim to hack, and the potential damage they could cause. Also, the authors in [14] adopted OCTAVE Allegro methodology to collect all security threats found by assessing the information security risk. The results of this research gave a better understanding and identified potential risks and security threats in an IoT-based smart home environment, summarized as: identity and credential theft, user's impersonation, malicious software, information modification, DoS, function and physics interruption, authentication. All these attacks can be performed due to different motivations, as described in [15].

One of these is that IoT is a new era in computing, so for attackers, it seems like a very interesting subject because of the immaturity of the products and protocols used in current IoT products. In addition, implementing IoT in the smart home is particularly vulnerable to privacy and security issue, such as weak authentication and encryption mechanism.

3. Possible related threats

Security is one of the main obstacles towards the wide adoption and diffusion of IoT applications. A research study has estimated that 80% of IoT devices are vulnerable to a wide range of hacks [16]. Attackers can exploit the following vulnerabilities to impact an IoT environments (e.g., a smart home) at various levels (application, network and perception layers):

- **Heterogeneous devices**: smart home devices are highly varied, each with different functionalities and purposes, as well defined in [17].Various sensors collect user habits, others monitor room occupancy, adjusting temperature and lighting and even optimize energy usage by learning patterns of activity. In addition, RFID can be integrated into a door locks, enabling the entrance automation. All these sensitive collected data poses challenges for ensuring secure connection while providing as many interactions and services as possible.
- **Limited authentication and authorization**: some IoT devices do not require proper authentication, others implement basic native mechanisms, relying only a username and password, for instance the MQTT application protocol, which opens the door to potential attacks.
- **Outdated Protocols**: many existing devices operate on protocols that lack necessary integrity, scalability, and interoperability. These protocols either do not implement or use weak access control mechanisms, compromising authorization for accessing certain resources. This lead to unauthorized access, resulting in data breaches and significant security issues.
- **Weak encryption**: if data transmitted or stored by devices is not properly encrypted or covered by small encryption key, it becomes transparent and easy for attackers to intercept, crack and exploit sensitive information.
- **Resource constraints**: devices are constrained by limited computing power, energy availability and storage capacity. These limitations make it challenging to implement robust security measures, leaving them susceptible to attacks.
- **Insecure applications**: there is a notable absence of systematic techniques for ensuring the privacy of IoT applications and middleware platforms. In addition, due to IoT limitations, developers often don't implement techniques to validate firmware integrity during installation, execution or upgrades, creating static and rarely updated "embedded software". Therefore, device may be vulnerable to malicious code that can infiltrate and merge with installed application software, providing attackers opportunities to execute harmful threats.

To secure any system, it is necessary to analyze the types of threats that will be faced, and how the threats will affect the systems security. The following subsections outline the main threats that can influence each layer and impact on the overall IoT environment.

3.1 Brute Force attack

A brute force attack is a method where an attacker systematically tries all possible combinations of passwords or encryption keys until the correct one is found. In the IoT environment, this technique can be particularly effective due to the often-weak encryption and straightforward authentication mechanism that are commonly implemented in these devices.

Imagine a smart home equipped with various IoT devices, interconnected through a central smart hub, which allows users to control them via a smartphone app or a web interface. The systems use a combination of username/password authentication and weak encryption protocols for data transmission with short keys, that can be easily broken with modern computing power. The attacker, thanks to automatic tools like Haschat, Hydra, Medusa, after identified the smart hub's IP address, can tires all possible combination, probabiy finding the correct credential to steal or decrypt sensitive credential. Consequently, with access to the smart hub, the attacker can control all connected devices, unlock doors, disable security cameras and manipulate the entire ecosystems.

3.2 Shadow Server

Shadow server refers to techniques involving attacks such as DoS and IP spoofing. In the context of IoT it leverages its capabilities to exploit vulnerabilities across both network layer and application layer. For the smart home scenario, a server is required to provide the necessary infrastructure to host the system and distribute content. Imagine, in the "worst-case scenario", that user is required to provide both credentials and a two-factor authentication to access control of their devices. The first step of this attack involves disrupting the primary infrastructure by overloading the systems with a DoS attack. Subsequently, the aim is to trick the unsuspecting user into entering their credentials and two-factor authentication on a malicious server specifically set up by the attacker. In more detail, through IP spoofing, an attacker could send a network packet with a spoofed IP address, pretending to be a trusted source. This enables unauthorized access and the acquisition of previously inaccessible information. Additionally, this technique can be used to mask the attacker's identity, making it difficult to trace the origin of the attack and facilitating malicious activities.

3.3 Man-in-the-middle

The initial step of capturing and examining traffic is crucial for attackers to understand the network's behavior and plan further malicious activities, such as injecting malicious code or gain access to the data. Attackers might employ various types of hardware or software, such as the Wi-Fi Pineapple or Ettercap, which can, for example, spoof legitimate access points and intercept underlying communication. This technique is often used to launch man-in-the-middle attacks, where the attacker positions themselves between the user and the network.

3.4 DoS

Denial of Service (DoS) attack is widely considered to be an important security issue [18]. It aims to make devices or network resources unavailable by flooding the network with useless traffic, exhausting resources or jamming signals. This attack prevents communications, compromise traffic, and waste resource, effectively blocking access to IoT services. While DoS attacks typically do not alter transmitted data, they can be launched remotely using specific tools and commands. The situation, as extensively described in [19], escalates if both data sources and the IoT platform are targeted. A saturated IoT platform, for example, with external request, cannot respond to legitimate ones promptly, causing slow communications and further damage related to storage and computational resources of both device and IoT platforms.

3.5 Packet sniffing

Due to IoT heterogeneous architecture in the smart home infrastructure, an attacker might use numerous programs and techniques to capture the traffic in the network among the different components of IoT devices, based on the attacker's capabilities and location [20]. Attackers often use tools like tcpdump or Wireshark to capture and examine the data packets transmitted over a network.
Packet sniffing is a specific technique used to compromise data confidentiality, by analyzing network traffic and allowing to monitor communication between devices, identify

patterns of activity and potentially access sensitive information. In a smart home environment, packer sniffing can be used in various ways: an attacker could intercept video streams from surveillance cameras within the home, for example.
By capturing the packets, he can view live feeds or recorded footage intended for security purpose, compromising the privacy and security of occupants. It is possible also monitor packets related to presence detection sensors or devices, in this way attackers can analyze this data to learn occupancy patterns, determine when occupants are away, or track their movements within the home.
Finally, since smart devices implements speakers or voice assistants to process voice commands and retrieve information, packet sniffing could intercept these interactions, capturing audio data or sensitive commands issued by users.

3.6 Packet Injection

Packet Injection is a technique where an attacker sends unauthorized packets into a network. This involves crafting and sending packets that appear to be part of legitimate communication session. The goal is to interfere with or manipulate the data being transmitted over the network. For example, inside a smart home, device often communicate with each other to perform automated actions based on user preferences or environmental conditions. Attackers could potentially manipulate the signals, such as commands to adjust lighting, temperature or appliance settings to disrupt normal operation or gain unauthorized control over home devices.

3.7 Trojan Horse

Due to the lightweight and autonomous version of well-known operating systems and firmware used in IoT devices and the lack of strong access control implementations, attackers can exploit these systems to access private information. Malware, particularly Trojan Horse, can be injected into IoT applications or systems, masked as a legitimate program. It is a malicious code hidden inside a file, link, etc.
Once downloaded by the user, it will execute the task the attacker designed it for, such as spy on users ‘online activity, open backdoor or steal sensitive data.

4. Possible related solutions

The complexity of managing security within IoT network is not limited to its implementation. Still, it extends to the need to find the right balance between the level of desired protection and the performance achieved.
The are currently several traditional security approach to preventing and limiting the risk of threats but many of them are not applicable in all IoT scenarios. For example, not all IoT devices are able to perform some types of cryptographic-mathematical computation, or they are not able to complete them in acceptable times.
The goal of security within IoT systems is not only to avoid the violation of confidential information or prevent access to malicious entities which could be simply interested in taking control over the device for very different purposes. Hence, the importance of ensuring security within IoT systems, from the physical to application level, become evident. So, traditional techniques could be revisited with respect to the dynamicity and heterogeneity of the IoT environment. In order to guarantee proper levels of security, an IoT system should provide authentication for:

- Data source: the entities that send data to the IoT platform (e, g., WSNs, WMSNs, RFID, social networks).
- Data request: the entities that require information to the IoT platform, in the form of services.

Then it should also provide encryption mechanism for ciphering the transmitted data and, to do this, adopts an effective key management system. Finally, policies able to regulate the access to the available resources should be defined and enforced.
However, besides such countermeasures would improve the resilience of the IoT systems, it is also essential to integrate security techniques that protect the entire systems and their interactions, from the

network to the user, improving the robustness of the system.
Before introducing advanced techniques that must be integrated into IoT devices, adhering to the by-design principle, it is essential to adopt core techniques that are simple, intuitive, and can be regularly applied during user interaction. Users can significantly enhance the security of their IoT systems by performing actions such as updating software, using private networks, applying up-to-date protocols, changing credentials frequently, backing up significant information and monitoring the network. In addition, other techniques are focused on the development side, where researchers and security experts are continuously studying and searching for new alternatives, considering the limitations of IoT devices.

4.1 Middleware

The primary reason for implementing middleware is to manage the heterogeneity of technologies used in IoT systems. IoT devices utilize a wide range of protocols and communication technologies that need to be integrated and manages securely and efficiently, Middleware can unify these technologies, ensuring interoperability and data protection. Many existing middleware solutions fails to comprehensively address security, privacy and data quality issues in IoT context. Beyond security, it's crucial to evaluate the quality of data collected by IoT device. NoS (Node-oriented-Service) middleware presented in [2] is designed to manage a large amount of data from heterogeneous devices with lightweight modules and interfaces that operates non-blockingly to perform data analysis and query, giving, in an asynchronous way, data to users, in form of services. The main functionalities of NoS are:

- Key management system: the architecture is integrated with algorithms used to manage the keys.
- Quality of Protection and data quality algorithms: automatic reasoning techniques are used to evaluate the QoP and DQ, by giving a score based on:
    - Authentication
    - Integrity
    - Confidentiality
    - Privacy
    - Completeness
    - Timeliness
    - Precision
    - Accuracy
- Policy Enforcement mechanism: it designs a flexible policy enforcement framework for handling violation, by:
    - Controlling the access of both user and data sources.
    - Controlling the data provision to users.
- Authenticated Publish/Subscribe system: the authentication of nodes is guaranteed by a system that includes a framework to handle the keys and the application of policies, solving the limitation of MQTT protocol.
- Policy Synchronization system: it integrates a solution to have distributed NoS with the same functionalities and policies to avoid the single point of failure and bottleneck issues introduced by a single centralized NoS.

4.2 Risk assessment

Conducing a risk assessment is crucial. It's a systematic process of identifying, analyzing, and evaluating potential risks associated with a system, process or activity, assessing the likelihood and impact of various risks to determine their significance and prioritize them for mitigation. IoT platforms generally fails to guarantee proper security controls or a well-defined assessment of the risk to which the systems may be exposed. It's challenging to identify a standardizes risk methodology that developers can uniformly apply, where they are focusing on three final goals: assessing how much users should believe in the systems trustworthiness, revealing weakness of the existing platforms, and evaluating possible countermeasures or improvements of the actual system components, in order to make the platform more resilient towards malicious attacks.

A possible flexible and robust approach is described in [21] where the risk analysis considers both static and dynamic features/components of an IoT system and aims to reveal the existing risks at the different levels of the data flow, reaching the goals before listed. However, with the rapid proliferation of cyber-physical systems, the validity of current approaches is being questioned. The cause lies in the heterogeneous nature of the actors involved: from the physical components responsible for executing specific mechanical movements, to the terminals forwarding commands related to these routines, and the personnel tasked with maintaining these digital and pyshical aspects. An effective risk assessment must be capable of identifying not only the inherent weaknesses of each individual entity but also those arising from direct and indirect interactions with other systems components, whether they involve human, cyber or pyshical relationships. This approach is defined 'hybrid', and TAMLESS [22] is one of the effective tools that analyze systems vulnerabilities considering these three different aspects.

4.3 Strong encryption

Using robust and dynamic standard encryption algorithms it is possible that when they are applied, the IoT devices shut down due to lack of energy, for example. Therefore, protocols are needed that can meet the "limitation" of these devices, such as sensors, whose role within the smart home is essential to collect information, process and share data. The SETA protocol [23] guarantees integrity, confidentiality, traffic congestion control, privacy and power saving by employing various technologies to ensure security and network longevity. The protocol is designed to address these requirements by employing a hybrid architecture that combines Wireless Sensor Network (WSN) with Wireless Mesh Network (WMN). This approach offers several advantages: the hybrid architecture allows sensors to do not perform aggregation and controls, saving power, while Mesh router conduct more accurate controls, reporting the security errors by indicating the affected nodes. Sensors are organized into clusters, performing different tasks and communicate with a cluster head, a more powerful node called Mesh, which is responsible to communicate with the sink node. Finally, the end-to-end secure data aggregation ensuring that data transmitted from sender to recipient within the network is securely aggregated. This is achieved by using homomorphic encryption, which allows encrypted data to be collected and sent inside the network without decryption. The decryption key is held by the sink, which handles the final decryption.

4.4 Robust DoS mitigation

The paper [19] presents a solution designed to actively and dynamically detect and mitigate DoS attacks within IoT systems. REATO (REActing to denial-of-service attacks) aims to provide a dynamic response to this type of attack, through detection and response: after identifying unusual traffic patterns indicative of a DoS attack, it implements countermeasures to mitigate the impact of the detected attack, enhancing the security and reliability of IoT applications. The robustness and performance validation of REATO is assessed by considering different crucial metrics, inside a real-world prototype, such as storage occupancy, CPU load and data retrieval delay.

4.5 Intrusion detection Systems

IoT is a tremendous network based on connected smart devices. However, these networks are at high risk in terms of security violations. An Intrusion Detection System (IDS) is essential to monitor and analyze network traffic for signs of malicious activity or policy violation. The primary function is to detect potential security branches, including unauthorized access attempts. IDS uses various detection methods to identify potential threats. One of these can be anomaly-based, it establishes a baseline of normal network behavior and flags deviations from this baseline as a potential threat. This method is effective for detecting unknown attacks but can produce false positive if normal behavior varies widely.

To address this problem, an hybrid approach design [24] is used, combining machine learning (ML) and deep learning (DL) techniques, enhancing the detection accuracy and reduce the misclassification rates.
The robustness is achieved by including a meticulous process of feature selection and hyperparameter tuning to address overfitting and underfitting issues, performing optimally under various condition, as demonstrate by the great applicability and effectiveness in the proposed smart home scenario.
Overall, an IDS is a crucial component of a comprehensive security strategy, helping detect and respond to threats in real-time to protect network infrastructure and sensitive data.

4.6 Solid access control mechanisms

Attribute-Based Encryption is a technique that combines cryptographic methods and access control mechanism allowing data to be encrypted for multiple recipients. The decryption is possible only if the recipient's attributes satisfy a defined access policy. Two different types can be applied, as described in [25]. Chipertext policy (CP-ABE) and Key policy (KP-ABE) where respectively, the chipertext/private key is associated with a policy on the presence of some attributes in the private key/chipertext. Each approach includes high customization due to variety of attributes that can be defined, providing a fine-grained access control, high security and flexibility, since data are secured both at rest and in transit. Additionally, ABE requires more resources, but can be less energy-intensive compared to traditional cryptographic methods, showing that it can efficiently menage memory occupancy and reduce delays in data retrieval, making it suitable for IoT applications.
In order to solve the problem of resources required, an alternative approach is the implementation of Sticky policies [25], which involves attaching access control policies directly to the data. These policies are evaluated and enforced by a trusted authority. The enforcement of access control rules is decentralized, which helps in spreading the load and avoiding single point of failure. As ABE, policies can be highly customized. This approach reduces the workload on the IoT platform improving overall efficiency.

5. Conclusion

As IoT adoption expands across different application domains, there is a rising need for solution that handle diverse devices while balancing convenience, comfort and data quality. However, this rapid integration has also highlighted serious challenges related to privacy and security, which remain key barriers to the widespread implementation of IoT on large scale. One major obstacle is the lack of a unified vision regarding the assurance of security and privacy requirements in these heterogeneous environments. To address this, there is an immediate need for solutions that are platform-independent and capable of guaranteeing confidentiality, integrity, access control, and privacy for both users and devices. Engineers and cybersecurity experts must consider all possible scenarios, including attacks on data source and the IoT platform itself. The approach must encompass cyber, physical, and human aspects, as well as the relationships between these components and the system's architectural elements.
This paper discussed the main vulnerabilities of IoT systems, particularly in the smart home domain, focusing on potential attacks, best practices and suggested solutions for enhancing overall security. Moving forward, it is imperative to design and deploy suitable security solutions that address the unique challenges posed by the different and interconnected nature of IoT devices. Only through comprehensive and integrated security strategies can we fully realize the potential of smart homes while safeguarding the privacy and security of users.

References

[1] S. R. A. G. L. A. &. C.-P. Sicari, «Security, privacy and trust in Internet of Things: The road ahead.,» *Computer networks,* n. 76, pp. 146-164, 2015.

[2] A. R. D. M. C. C. A. C.-P. Sabrina Sicari, «A secure and quality-aware prototypical architecture for the Internet of Things,» *Information Systems,* vol. 58, pp. 43-55, 2016.

[3] C. S. W. H. M. B. G. C. Thomas Kothmayr, «DTLS based security and two-way authentication for the Internet of Things,» *Ad Hoc Networks,* n. 11, pp. 2710-2723, 2013.

[4] W.-C. L. Y.-H. H. J.-Y. Lee, «A lightweight authentication protocol for internet of things,» *International Symposium on Next- Generation Electronics,* pp. 1-2, 2014.

[5] Y. Z. R.-c. W. R. M. L. Q.-m. Ning YE, «An Efficient Authentication and Access Control Scheme for Perception Layer of Internet of Things,» n. 4, pp. 1617-1624.

[6] Z.-Q. WU, Y.-W. ZHOU e J.-F. MA, «A security transmission model for internet of things,» *Jisuanji Xuebao(Chinese Journal of Computers),* n. 8, pp. 351-1364, 2011.

[7] G. B. L. G. G. Piro, «A standard compliant security framework for ieee 802.15.4 networks,» *Proc. of IEEE World Forum on Internet of Things (WF-IoT),* pp. 27-30, 2014.

[8] D. E. D. Evans, «Efficient data tagging for managing privacy in the internet of things,» *Efficient data tagging for managing privacy in the internet of things,* pp. 244-248, 2012.

[9] R. F. B. C. T. Z. A. R. X. Huang, «User interactive internet of things privacy preserved access control,» *7th International Conference for Internet Technology and Secured Transactions,* p. 597–602, 2012.

[10] B. C. E. F. K. T. J. Cao, «CASTLE: continuously anonymizing data streams,» *IEEE Trans. Dependable Secure Comput,* n. 3, p. 337–352, 2011.

[11] J. I. a. N. Y. I. G. Seissa, «Cyberterrorism Definition Patterns and Mitigation Strategies: A Literature Review,» *Int. J. Sci. Res.,* vol. VI, n. 1, p. 180–186, 2017.

[12] I. K. R. N. I. N.-F. G. S. a. G. B. D. Geneiatakis, «Security and privacy issues for an IoT based smart home,» *0th Int. Conv. Inf. Commun.Technol. Electron. Microelectron,* p. 1292–1297, 2017.

[13] S. M. S. M. K. T. P. a. N. H. A. J. H. Awan, «Cyber Threats/Attacks and a Defensive Model to Mitigate Cyber Activities,» *Mehran Univ. Res. J. Eng. Technology,* vol. XXXVII, n. 2, p. 359–366, 2018.

[14] B. A. a. A. I. Awad, «Cyber and physical security vulnerability assessment for IoT-based smart homes,» *Sensors (Switzerland),* vol. XVIII, n. 18, pp. 1-17, 2018.

[15] M. S. a. F. E.-M. D. Bastos, «Internet of Things: A Survey of Technologies and Security Risks in Smart Home and City Environments,» *IET Conference: Living in the Internet of Things: Cybersecurity of the IoT,* p. 30, 2018.

[16] «Rambus,» [Online]. Available: https://www.rambus.com/iot/smart-home/.

[17] C. &. B. M. &. B. A. Badica, «An overview of smart home environments: Architectures, technologies and applications,» *CEUR Workshop Proceedings,* n. 1036, pp. 78-85, 2013.

[18] S. &. J. J. &. T. D. Taghavi Zargar, «A Survey of Defense Mechanisms

Against Distributed Denial of Service (DDoS) Flooding Attacks,» *IEEE Communications Surveys &amp Tutorials,* n. 15, pp. 2046 - 2069, 2013.

[19] S. &. R. A. &. M. D. &. C.-P. A. Sicari, «REATO: REActing TO denial of service attacks in the Internet of Things,» *Computer Networks,* n. 137, 2018.

[20] K. N. N.-F. S. B. Geneiatakis, «Security and privacy issues for an IoT based smart home,» 2017.

[21] S. &. R. A. &. M. D. &. C.-P. A. Sicari, «A Risk Assessment Methodology for the Internet of Things,» *Computer Communications,* n. 129, 2018.

[22] F. &. K. E. &. S. R. &. L. E. Valenza, «A Hybrid Threat Model for Smart Systems,» *IEEE Transactions on Dependable and Secure Computing,* pp. 1-14, 2022.

[23] S. &. G. L. &. R. A. &. B. G. &. C.-P. A. Sicari, «SETA: A SEcure sharing of TAsks in clustered wireless sensor networks,» *International Conference on Wireless and Mobile Computing, Networking and Communications,* 2013.

[24] N. &. S. A. &. Q. K. &. H. S. &. O. A. &. B. F. &. A. N. Butt, «Intelligent Deep Learning for Anomaly-Based Intrusion Detection in IoT Smart Home Networks,» *Mathematics,* n. 10, p. 4598, 2022.

[25] S. &. R. A. &. D. G. &. P. P. &. M. M. &. C.-P. A. Sicari, «Attribute-based encryption and sticky policies for data access control in a smart home scenario: a comparison on networked smart object middleware,» *International Journal of Information Security,* n. 20, pp. 1-19, 2021.