electronics

MDPI

Review

Review of Smart-Home Security Using the Internet of Things

George Vardakis [1], George Hatzivasilis [2,*], Eleftheria Koutsaki [1] and Nikos Papadakis [1]

[1] Department of Electrical and Computer Engineering, Estavromenos Campus, Hellenic Mediterranean University, 71410 Heraklion, Greece; vardakisyageorge@yahoo.com (G.V.); eleftheria_koutsaki@yahoo.com (E.K.); npapadak@cs.hmu.gr (N.P.)

[2] Department of Electrical and Computer Engineering, Kounoupidiana Campus, Technical University of Crete, 73100 Chania, Greece

* Correspondence: gchatzivasilis@tuc.gr

Abstract: As the Internet of Things (IoT) continues to revolutionize the way we interact with our living spaces, the concept of smart homes has become increasingly prevalent. However, along with the convenience and connectivity offered by IoT-enabled devices in smart homes comes a range of security challenges. This paper explores the landscape of smart-home security. In contrast to similar surveys, this study also examines the particularities of popular categories of smart devices, like home assistants, TVs, AR/VR, locks, sensors, etc. It examines various security threats and vulnerabilities inherent in smart-home ecosystems, including unauthorized access, data breaches, and device tampering. Additionally, the paper discusses existing security mechanisms and protocols designed to mitigate these risks, such as encryption, authentication, and intrusion-detection systems. Furthermore, it highlights the importance of user awareness and education in maintaining the security of smart-home environments. Finally, the paper proposes future research directions and recommendations for enhancing smart-home security with IoT, including the development of robust security best practices and standards, improved device authentication methods, and more effective intrusion-detection techniques. By addressing these challenges, the potential of IoT-enabled smart homes to enhance convenience and efficiency while ensuring privacy, security, and cyber-resilience can be realized.

Keywords: smart home; security; privacy; resilience

Citation: Vardakis, G.; Hatzivasilis, G.; Koutsaki, E.; Papadakis, N. Review of Smart-Home Security Using the Internet of Things. *Electronics* **2024**, *13*, 3343. https://doi.org/10.3390/electronics13163343

Academic Editor: Hung-Yu Chien

Received: 26 June 2024
Revised: 14 July 2024
Accepted: 19 July 2024
Published: 22 August 2024

1. Introduction

Over the past few decades, significant advancements have been made in computer science, especially in the realm of utilizing and accessing the Internet [1,2]. Nowadays, virtually all modern-day activities involve the use of Internet-related services [3,4]. In more recent times, the use of Internet of Things (IoT) services has rapidly permeated our lives [5,6]. With this technology, a fully automated environment is being created, or at the very least, efforts are being made aimed at creating it. This is accomplished by utilizing the Internet and smart devices, including but not limited to smartphones, home assistants, smart TVs, watches, doors, thermostats, vacuums, and more. Figure 1 depicts the main elements of an IoT ecosystem.

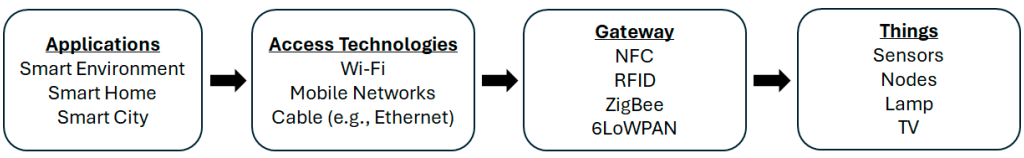

Figure 1. Basic building blocks of IoT ecosystems.

These smart devices utilize similar sensors that collect data and collaborate with one another to establish an automated environment that furnishes a diverse range of services to

modern society. These services provide convenience, speed, and security, particularly in the context of smart homes. A study conducted by Cisco [7] underscores the exponential growth of personal Internet-enabled devices. Specifically, in 2010, there were 12 billion connected devices; in 2015, there were 25 billion; in 2020, there were 50 billion; and it is projected that by 2035, the number of Internet-connected devices will reach 1 trillion.

The IoT takes advantage of the growing trend of interconnected devices to offer a wide range of services through a single device, such as the user's mobile phone. However, managing and securing a home through IoT technology is a significant challenge due to the heterogeneous and independent technologies of the devices. Although there are numerous smart-home devices available that offer individual services to users, these devices must interact and cooperate with one another, which can be a major obstacle due to the different technologies and protocols they employ. This heterogeneity makes them vulnerable to attacks and creates an insecure environment. The ISO-27005 security protocol [8] identifies the vulnerabilities of a connected-device environment that can cause a total system failure in terms of security, allowing malicious, unauthorized users to intrude into the network and gain access to all of the personal data and management services provided through the network remotely. In 2014, for example, videos from 73,000 Internet-connected cameras were leaked online, and in 2016, every Internet-connected device was attacked, on average, once every two minutes [9]. According to research by HP [10], approximately 70% of smart devices are vulnerable to threats, and during the trial stage, 90% of the personal data collected during the installation of smart devices were intercepted.

In this digital era within which we are living, technology is progressing at a fast pace and is interleaved within our daily activities. Modern cyber–physical systems are materializing new applications and are providing a way of living which would have seemed quite futuristic some decades ago. Smart homes, and smart spaces in general, are one such novel installation and the main focus of this paper. Advance automations, AI, assisting with living, safety, and even robotics and personalized healthcare, constitute some indicative use cases. More and more people are becoming familiarized with these settings and are deploying them in their houses and/or other smart environments (e.g., hotels, workplaces, factories, etc.).

The human is now a core part of this cyber loop. In the role of the system user, he/she is now the main "subject" of these, usually personalized, ecosystems. Therefore, the protection of residents, from both cyber threats and potential physical threats, is of paramount importance.

However, the underlying technologies and their interplay in such complex systems make it hard to safeguard them. The IoT; cloud services; the high variety of smart devices, sensory equipment, and networking options; electronic and mobile commerce; social media; and AI form some of these elements. Their evolution has proceeded so quickly during recent years that regulatory efforts, as well as the conscious and mature usage of technology, have fallen behind. Governmental and standardization efforts are seeming to progress very slowly, as they require many years to produce results, and when they do, the technology has progressed further on. Users' awareness is low concerning the dangers underneath; the adaptation of these applications is not mature enough; and, in the event, the market and private sector does not have the required numbers of experts (like technicians and engineers) to support them.

Therefore, there are several challenges for smart-home security, including the following.

- User awareness level: Users are always considered one of the weak links on the cyber risk chain, and usually, home users are not aware of the cyber threats related to smart-home devices, or may not know how to properly secure them. This can lead to weak passwords, false configurations, failure to update software, and other security vulnerabilities.
- Complexity: Smart homes can be complex systems with many devices, sensors, and services. This complexity can make it difficult to manage security and identify vulnerabilities.

- Interoperability and Heterogeneity: Smart-home devices are often developed by different manufacturers and use different communication protocols, which makes it difficult to ensure that they can all work together securely.
- Remote access: Smart-home devices often allow for remote access via Internet connection, which increases the risk of unauthorized access by attackers. This is especially concerning as many users may not secure their remote access properly.
- Limited resources: Smart-home devices often operate with limited resources, such as low power consumption, limited memory, and processing power. This makes it challenging to implement strong security protocols.
- Lack of regulation: There are currently no standardized security regulations for smart-home devices, which means that security measures can vary widely between different devices and manufacturers.

This paper will analyze the security issues in a home environment and propose solutions to address them [11–14]. Since almost everything works or uses the Internet, users have a significant responsibility to educate themselves about the proper and safe use of their smart devices and the associated risks and threats [15–18]. Modern modeling approaches consider that the IoT technology comprises four layers (application, perception, network, and physical) [19], each of which is susceptible to different types of attacks, and this paper will examine these attacks by layer and provide recommendations for dealing with them. Moreover, in contrast to similar works, this review also examines the particularities of popular categories of smart devices, like home assistants, TVs, AR/VR, locks, sensors, etc.

The rest of the paper is structured as follows: Section 1 introduces the concept of cyber security in modern smart-home IoT environments. Section 2 presents related surveys. Section 3 describes the modern smart-home ecosystem and the various IoT devices that can be found within it. Section 4 analyses the architecture of the IoT setting and reviews the attacks, countermeasures, and challenges for securing a smart home. Section 5 discusses the findings of this work and proposes security guidelines to safeguard the various components and system layers of smart homes. Section 6 highlights directions for future research. Finally, Section 7 concludes this study and refers to future works.

2. Related Works

Research studies have led to the implementation of rules that are crucial for system security and the protection of private information [14,20,21]. The vulnerabilities of the IoT architecture were identified, such as the heterogeneity of smart devices and their Internet interaction, which can potentially expose a home's security to intruders [22–24]. Preventing future threats and identifying solutions for possible system attacks are the main concerns of these studies.

Yang and Sun [25] offer an extensive examination of the security challenges facing smart-home systems. This research delves into the architecture of smart homes, identifying six natural and contextual features, and discusses the dichotomy of "spears" (cyber-attack methods) versus "shields" (countermeasures). The paper highlights various security frameworks and evaluation technologies and discusses the integration of smart-home technology with other fields, such as blockchain, cloud computing, and artificial intelligence. The authors suggest that future research should focus on unifying architecture, addressing resource limitations, managing fragmentation, and enhancing code and firmware security. The survey also emphasizes the importance of prioritizing security in smart-home research over the commercialization process to ensure the development of robust and reliable systems.

Dahmen et al. [26] provide a comprehensive overview of how smart-home technologies contribute to security. The authors explore a range of smart-home functionalities that enhance the safety of residents, including the detection, identification, and response to potential threats. They offer a comparative analysis of both existing commercial products and academic research in the field. Key contributions include the discussion on sensing

mechanisms within smart homes that detect anomalies or security breaches, assessing the nature and severity of these threats, and the automated response systems designed to manage these threats effectively.

Bastos et al. [27] thoroughly examine the integration and implications of IoT technologies within the home. The paper addresses how devices are becoming ubiquitous in households, expanding the IoT landscape but also escalating security vulnerabilities. It highlights the significant increase in IoT-device deployment and the corresponding security expenditures forecasted to manage associated risks. The study details various IoT components, including sensors, actuators, and network protocols, emphasizing their roles in enhancing connectivity but also in increasing potential security breaches. The authors discuss current security challenges, such as the susceptibility to Distributed Denial of Service (DDoS) attacks and the ease of unauthorized access due to weak authentication practices. The paper concludes with a call for robust security measures embedded within the IoT development phase and continuous updates to safeguard a system against evolving cyber threats, aiming for a secure integration of IoT into daily life and infrastructure.

Researchers are particularly focused on identifying solutions for intrusion-detection systems (IDSs) for smart homes [28,29], which are critical for protecting the security of the system. The quality of service of the network is also a major issue that must be addressed in order to ensure system security. Software-Defined Networks (SDNs) offer scalability of the system, but they also increase the system's vulnerability to attacks. Researchers are tasked with developing solutions that protect the security protocols [30–32] of Routing Protocol for Low-Power and Lossy Networks (RPL) and IPv6 over Low-Power Wireless Personal Area Networks (6LowPan) from possible attacks, while maintaining a secure network and high quality of service (QoS). In addition to a high QoS value, the IDS performance must remain sufficient, with low energy consumption and a low data processing time, while also ensuring an immediate response. Despite the significant requirements for IDSs, the convenience that IoT systems provide for home security makes researchers persist in identifying solutions to the problems that IDSs face [23–28]. Radio Frequency Identification (RFID) technology offers an important contribution to IDS security by facilitating the interfacing of smart devices in a smart home [33]. This article will delve into the security issues and technologies identified for smart homes, starting with an analysis of the architecture layers of an IoT system. The heterogeneity of smart-home devices is a major weakness of the IoT system [24,34,35].

A suggested solution for ensuring a safe home environment involves the use of a Wireless Sensor Network (WSN) that utilizes IoT technology to provide various services [36–38]. The sensors in the network detect and track movements and interact with each other to provide useful information to the system. Researchers are studying WSN to ensure the privacy and security of the entire home environment, as there are threats and attacks that can be received by a smart home using IoT technology. The proposed solutions are categorized based on the threats and attacks that the system can face. However, the privacy and confidentiality of information remain a significant challenge for researchers. The rapid development of intelligent devices, particularly mobile devices, is not keeping pace with the development of protocols and security systems, which means that these devices are increasingly used in IoT technologies without the required security and protection of the system [39]. Therefore, the creation of smart devices supported by strong security protocols should be the first concern to ensure the security and privacy of the smart-home environment. In this environment, all smart devices interact with each other automatically, and the data managed by each device are sent to a central unit to process. The system should be able to detect potential malicious devices that attempt to gain access to it by pretending to be part of the legitimate system. The heterogeneity in the interface options of smart devices is a significant issue that needs to be solved by defining a sufficient architecture with strong protection protocols. This creates the need for research into security, integrity, confidentiality, and energy-efficient methods [27,40]. The IoT mainly consists of devices that operate with low power and small memory, which requires the system to respond with

the lowest possible computing power and energy consumption. However, sending data to the cloud or the fog layers can open a huge portal for the interception of this data, while natural disasters, such as a fire, can cause the system to collapse. The different security protocols and capabilities of different devices also pose a challenge to the cooperation and compatibility of the system. The system is susceptible to different type of attacks based on the related layers of the IoT architecture, which are analyzed in the following sections.

Other surveys are examining not the smart-home environment itself, but specific types of devices. For example, Xu et al. [41] studied the security of home assistants, Santani et al. [42] examined smart TVs, and Guzman et al. [43] analyzed mixed-reality solutions.

This study takes into account modern design approaches (e.g., [19]) that decompose the analysis of a smart-home system into four layers (application, perception, network, physical) and propose a unified architecture. Moreover, this research is not just an analyses of the generic IoT features and their security implications, but also examines a series of equipment and solutions that can be actually found in a home environment. This includes analysis of the security particularities of smart-home assistants, TVs, AR/VR glasses, vacuums, locks, sensors, etc. To our knowledge, this is the first paper that researches the security implications of a quite complete list of smart-home devices and follows the modern smart home and IoT architectures.

3. Smart-Home Ecosystem

This section presents the various IoT devices that can be found in a smart-home system.

3.1. IoT in Smart Homes

A typical smart home consists of several IoT devices that are interconnected via a router-modem. This router is the main network device which undertakes the effort to connect all these devices at the edge system, as well as to enable communication with Internet and the cloud. The home devices rarely possess their own Internet connection, while the user can interact with this ecosystem through his/her smartphone, which has a direct broadband connection. Ordinarily, this router is the only barrier between the outworld and the private home. Therefore, its security and proper configuration are of paramount importance.

The devices can join Local Area Networks (LANs) formed by the router, either through an Ethernet cable or wirelessly. Some devices might support the direct link with the user's smartphone, e.g., via Bluetooth. Devices may expose services and APIs, either within the edge system or to the Internet. Their security and proper setting must also be examined carefully.

In modern settings, home assistants form one main device to interconnect IoT equipment. The home assistant connects to the router for Internet access, while IoT devices are connected wirelessly with the home assistant for local networking. The user administrates the system via his/her smartphone, tablet, or PC, which are connected (wired or wirelessly) with the home assistant, while the daily use/operation is driven by vocal commands. Home assistants are one of the most intelligent smart-home devices in modern installations [41]. They can also be deployed to administrate other less intelligent devices, like light and sound devices, and they may also be aware of the residents' preferences and personal information. Also, they constitute one of the main indoor interfaces for the user to interact with the home via vocal commands and without using a smartphone or other device. Therefore, home assistants are a targeted element of state-of-the-art attacks [44]. Assistants, like Google Home and Amazon Alexa, are vulnerable to attacks such as voice squatting [45,46]—where attackers use similar sounding phrases to trigger the device to perform unintended actions; and eavesdropping—where attackers can use the device to listen to private conversations. There have also been instances of malicious applications and phishing attacks targeting users of smart-home assistant devices. As these devices become more popular and are integrated into more homes, it is likely that there will be continued efforts by attackers to find new vulnerabilities and exploit them [47,48].

Smart TVs are quite common equipment in houses nowadays [49]. The TV receives the ordinary TV signal from an antenna or a cable and is connected to the Internet via the router (connected wired or wirelessly) for the "smart" content, while the user interacts with it through the telecontrol with RF signaling (application developers have also implemented such functionality for mobile devices, like smartphones) or with vocal commands via the home assistant [42]. In some cases, TVs have their own mike and camera sensors, and the user can directly interact with it via vocal commands or gestures. Other devices, like a keyboard or mouse, can be connected via Bluetooth. Also, the owner may be connecting his/her social-media or other accounts (e.g., YouTube or Netflix). However, the TV may also be used by other residents or guests, exposing the owner's privacy, as well as raising some security concerns [50–53].

Augmented Reality (AR) and Virtual Reality (VR) glasses [43] constitute another type of equipment that may be found in a smart environment, like a house. These devices can be connected wirelessly (i.e., Wi-Fi) to the Internet via the router. Usually, the user may be connected to his/her social media or another service (e.g., Facebook or Netflix). Similar concerns as for the smart TVs are raised. As for the home assistant and TVs, malicious applications may find their place in the related application stores. Moreover, in the case of AR, the user is experiencing augmented reality indoors during his/her daily activities and (remote) working hours. Therefore, in an augmented office environment, the glasses' camera would capture the computer's (or other device's) screen, including the user inputting his/her login information to various services and applications, as well as confidential and private conversations. Additionally, as a portable device, AR/VR glasses are easier to lose when the user takes them with him/her outside, or may even be stolen. Therefore, more advanced controls are required of the device-level security, e.g., remote deletion of data or blocking of the device.

Smart locks are installed in doors and windows to control their shielding [54]. The lock itself can be materialized via physical means as an ordinary lock or with magnetic solutions. Usually, someone can freely open from inside (also complying with safety requirements for cases like building evacuation or when electricity or Internet connection are cut off). To enter the private space, someone can unlock the equipment via various means, including control through the Internet and a related mobile application, performing a wireless challenge–response protocol with a smart phone, prompting a code in a pad, authenticating via biometric sensors, or using a card or other access token, as well as the ordinary use of a physical key (again for safety and dependability reasons). Moreover, smart locks constitute a popular solution for short-term hiring apartments (e.g., for the Airbnb and Booking platforms), where the owner produces new access codes/keys/tokens for every new client, as well as the cleaners or other tenders. Hotels and cruise ships are mostly in favor of using magnetic cards as access tokens to rooms and cabins, respectively. The security of smart locks is of paramount importance. Mostly, attacks are originated by criminals who want to gain physical access to the private space. The attackers might try to exploit vulnerabilities in the communication link and transmission of data, tampering physically with the equipment, overcoming biometric authentication, or performing social-engineering attacks to gain the access credentials.

Surveillance IP cameras are another popular feature of smart homes [55]. The cameras are gaining Internet access via the router (Ethernet or Wi-Fi connection) and are accessible from outside, usually via the user's smart phone and a related application. Ordinarily, the cameras record video and audio, and the communication is bidirectional, with the user being able to rotate the camera or talk through its speaker. However, most users are installing this system by themselves, leaving default configurations including default or no passwords to login and access the cameras [9]. Attackers may exploit this functionality to spot the residents' absence for physical assaults, record residents and violate or harm their privacy, or even talk to children and babies performing spooky pranks.

The smart vacuum is a preliminary robotic device that can be found in modern houses [56]. Vacuums have autonomous operation to scan the area and clean the available

space, and they can be controlled via an RF telecontrol. Smart vacuums may connect with the router for local Wi-Fi interaction or communication via the Internet. The user exploits these two options via his/her smart phone and a related application. Thereupon, the user can access more advance functionality, e.g., view a map of the scanned space and make adjustments, schedule cleaning operations, review historic data, etc. Thus, a vacuum may maintain sensitive information, like the house floor mapping and the indoor arrangement. In some cases, smart vacuums utilize a camera senor to navigate the floor and avoid obstacles, also capturing sensitive information from the home's inside, as well as the residents while living in their private space.

Other devices and sensors can be found in a smart environment. These may include lamps and lighting equipment in general [57] for the control of ambient light, thermostats [58] for heating water, and air-conditioning [59] for adjustment of the indoor temperature. Smart functionality can also be found in ovens [60] to monitor and control the cooking process or refrigerators [61] to record the stored goods and help in scheduling the resident's shopping routine. Smart plugs [62] form another device category that is gaining interest. These plugs are connected to the home's electricity grid, and ordinary devices are connected to the smart plugs. Smart plugs control the electric power on this equipment, performing smart-home functionality like open or close devices (thus starting or stopping the devices' actual operation). Usually, all these devices are managed via the user's smart phone and related applications. Once set, these installations are rarely monitored or maintained by their users in terms of security. Therefore, when equipment is compromised by attackers, it remains infected for long periods, with attacks like crypto-jacking or Denial of Service (DoS) campaigns to external victims going completely unnoticed [63,64]. Moreover, attacks on the related devices pose great threats to the safety and well-being of the residents, while they can also cause significant economic losses (i.e., excessive energy consumption and damaged equipment).

The disposal of smart-home devices introduces significant security implications and challenges [65], primarily due to concerns for data privacy and the potential for unauthorized access. Many of these devices, ranging from smart thermostats to home assistants, store sensitive user data which, if not properly erased before disposal, can be retrieved by malicious actors. This vulnerability presents a considerable risk, particularly with devices that lack a clear, user-friendly process for fully erasing stored data. Additionally, improperly disposed devices can still connect back to a user's network (e.g., if not correctly deregistered), allowing potential ongoing access to live data and network resources. These challenges highlight the need for robust data management practices, clear guidelines on device decommissioning, and awareness among users about the security risks associated with disposing of their smart-home equipment. The same conditions also hold in the case of the user selling the device.

The home resident is the main actuator who uses and, usually, installs the overall IoT ecosystem [66]. However, an arbitrary user would not possess the knowledge and expertise to set this system; thus, the awareness level of users must be enhanced. Although the home resident is the main actuator, other people might access the home network, like guests who receive Wi-Fi access to connect to the Internet or technicians who must install or repair some device. Moreover, in some cases like in hired apartments or hotels, even the residents of this smart private space can change, as well as the personnel that work within.

3.2. Infotainment Devices

The main home-assistant solutions are provided by large companies, like the Google Home, Amazon Alexa, Apple Siri, and Microsoft Cortana [67]. Ordinarily, these systems utilize Deep Neural Networks (DNN) and multi-modal dialogue systems for Automatic Speech Recognition (ASR), Natural Language Understanding (NLU), and the incorporation of gestures and visual input to create more interactive and engaging user experiences [67]. In the smart-home environment, these systems offer an easy-to-use setting for the average user and ease integration with compatible smart-home devices.

Fruchter and Liccardi [68] studied users' attitudes and concerns towards the security and privacy of home assistants, with only 2% of participants reporting problematic issues, like (i) data collection and scope, (ii) "creepy" device behavior, and (iii) violations of personal privacy thresholds. However, several security and privacy issues and challenges have been reported by researchers and practitioners [69–74]. Among others, these involve (i) the continuous processing of data by these devices and potential disclosure of private information to companies or adversaries, (ii) vulnerabilities in data transmission or storage mechanisms (e.g., an adversary outside the victim's house can connect his/her smartphone to the victim's Bluetooth speaker and then play an MP3 audio file of voice commands [69]), (iii) third-party exposure by the insufficient reviewing of applications in related application stores or insecure collaborating devices, which may inject vulnerabilities or weak security mechanisms into the home system, (iv) low security awareness by the user, who may not set or configure the system properly (e.g., use weak passwords or other authentication mechanisms), or maintain it (e.g., not updating or patching the system on a frequent basis), (v) attacks exploiting the open vocal interface [70], like mischievous neighbors or criminals speaking commands from outside, replaying commands via other means (e.g., TV commercials), commands in ultrasonic frequencies which cannot be heard by humans but can be detected by smart speakers, etc., (vi) challenges of supporting a multi-user environment, like protecting a user's private data from the rest of the users of the same smart environment (e.g., hired apartments, elder residents, or people with disabilities with support person dyads [71–73], etc.), or imposing smart-home ownership and control among family members (family rivalry) [74] or pets with talking capabilities (i.e., parrots or mynas [70]).

Home assistants, in their always-on listening capability, are designed to activate upon hearing a wake word. This feature, while convenient, raises the possibility of inadvertent recording and data collection [75]. There have been instances where conversations were recorded and transmitted without user consent due to false triggers or misinterpretations of the wake word. The storage and processing of vocal commands on remote servers further exacerbate privacy concerns, as any breach from these data centers could expose users' sensitive information.

Home assistants are linked to user accounts containing a wealth of personal information, including contacts, calendars, and even financial data. Attackers who gain access to these accounts can potentially hijack not only the home assistant but also other connected services. Weak or reused passwords, a lack of two-factor authentication, and phishing campaigns are common vectors for unauthorized access attacks.

Third-party applications from application stores or other sources also pose a security challenge. Home assistants allow the installation of third-party skills or applications that enhance functionality. However, these third-party integrations can be a source of vulnerabilities, especially if they are not properly examined for security threats. Malicious skills could perform unwanted actions, such as eavesdropping or sending data to unauthorized third parties.

Often, these devices serve as hubs for controlling other IoT equipment, such as locks, cameras, and thermostats. However, IoT devices are notoriously insecure, often lacking robust security features. An attacker who compromises a poorly secured IoT device could potentially gain access to the network and use it as an entry point to attack the home assistant or other more sensitive devices that are connected to the same network.

Regular updates are crucial for maintaining the security of home assistants by patching known vulnerabilities. However, delays in deploying updates or the discontinuation of support for older devices can leave them vulnerable to exploitation. Users may not always be aware of the need to update their devices or may be unable to do so if the manufacturer no longer supports their model.

To address these vulnerabilities, users and manufacturers must take proactive steps [70,76]. Users should regularly update their devices, use strong, unique passwords, and enable two-factor authentication where available. Additionally, users should be cautious about the

permissions granted to third-party skills and applications. Manufacturers need to prioritize security in the design and development of home assistants and connected IoT devices. This includes ensuring the secure storage and handling of voice data, providing timely security updates, and rigorously evaluating third-party integrations for security risks. Home-assistant manufacturers need to build robust voice authentication of the user/owner to counter voice-related attacks, as well as access and authorization policies for multi-user environments. For example, parents must have higher access privileges than their children, and the system must be able to understand when a child misbehaves and tries to annoy the parent (e.g., commanding the home assistant to play music, while the parent has said no).

Smart TVs [49–53], as integral components of the IoT ecosystem, have transformed entertainment systems into sophisticated interactive devices. They combine traditional television technology with Internet capabilities, offering users access to streaming services, applications, and smart-home control. However, their connectivity and processing capabilities introduce significant security and privacy concerns that must be addressed to protect users and ensure system integrity.

Smart TV architecture typically comprises several layers [49], including hardware, the operating system, middleware, applications, and connectivity interfaces. At the hardware level, smart TVs are equipped with processors, memory, and networking components that support Internet connectivity, usually through Wi-Fi or Ethernet. The operating system, often a version of Linux or Android, provides the necessary platform for running various applications and handling device operations. Middleware offers additional functionalities, like voice recognition and social media integration, while applications range from video streaming services, like Netflix, to interactive games.

The architecture of smart TVs includes complex components [49]: powerful processors, operating systems commonly based on Android, and multiple connectivity options including Wi-Fi and Bluetooth. Each component, while increasing the utility of smart TVs, also opens new avenues for cyber-attacks [50]. For instance, the integration of third-party applications can introduce risks if these applications are not properly evaluated for security. Moreover, the operating systems themselves can be prone to attacks if not regularly updated with security patches. Smart TVs are susceptible to a range of security threats and attacks, broadly categorized into the following: (i) remote attacks—where attackers exploit network vulnerabilities to gain unauthorized access; (ii) malware and ransomware—targeting operating systems and applications; (iii) data interception and leakage—where sensitive information such as user credentials and viewing habits is captured; (iv) physical attacks—including USB-based exploits to install malicious software; and (v) third-party applications and services—which may contain vulnerabilities or malicious functionalities.

One of the most concerning aspects of smart-TV vulnerabilities is their potential to be exploited for remote attacks [50,52]. Cybercriminals can gain unauthorized access to a TV's camera and microphone, spying on users without their knowledge. Similarly, because smart TVs often connect to other home devices, compromising a TV can lead to further breaches across a user's entire home network. Malware can also be a significant threat, as attackers may install malicious software to steal personal information, inject ads, or enlist the TV into a botnet for larger Distributed DoS (DDoS) attacks.

On the bright side, efforts to mitigate the risks associated with smart TVs have led to the development of various countermeasures and solutions [51,53]: (i) implementing robust encryption methods for data transmission and storage, (ii) utilizing multi-factor authentication or even biometric data to restrict access to the device, (iii) policies to ensure that the TV's firmware and applications are regularly updated to address known vulnerabilities, (iv) protecting the device's startup process and critical operations from tampering (e.g., secure boot and Trusted Execution Environment (TEE) functionality), (v) employing Artificial Intelligence (AI) and Machine Learning (ML) algorithms to detect unusual behavior that may indicate a security breach, and (vi) using techniques, such as differential privacy, to protect user data collected by applications.

Augmented Reality (AR) and Virtual Reality (VR) technologies being increasingly integrated into smart-home environments, enhancing the way users interact with their living spaces [43]. However, as these immersive technologies find their way into our homes, they bring with them unique security challenges and vulnerabilities that need to be carefully managed to protect user privacy and data security.

One of the primary security concerns in using AR and VR within smart homes is the potential exposure of sensitive personal information [77]. These technologies often require the collection and processing of large amounts of data to function effectively, including real-time location data, visual recordings from AR glasses or VR headsets, and biometric data to customize experiences. These data are highly sensitive, and if compromised, could be used for malicious purposes, such as identity theft, unauthorized surveillance, or targeted phishing attacks.

The challenge of securing user authentication in smart homes using AR and VR technologies is also significant [78,79]. Traditional authentication methods are less suited for these interactive environments and can be intrusive or disrupt the user experience. Newer methods, such as gesture recognition or eye-tracking, offer more seamless integration. Stephenson et al. [79] evaluated existing AR/VR authentication mechanisms and proposed a comprehensive framework for developing future methods that emphasize the user experience and security. They highlight the inadequacies of password systems and suggest the use of multimodal sensors available in AR/VR devices for authentication purposes. This includes novel approaches—such as behavioral biometrics using eye and head movements; and more advanced techniques—like skull and ear biometrics, which leverage the specific capabilities of AR/VR hardware to ensure user authenticity in a way that is both unobtrusive and secure. However, such approaches may introduce new vulnerabilities, such as the risk of behavioral biometrics being mimicked or intercepted by unauthorized parties. Moreover, the interaction methods used, like vocal commands or motion sensors, can be susceptible to eavesdropping or hijacking, leading to unauthorized actions or access within the smart home.

Another concern is the security of the devices themselves, which are often connected to the home's main network. This connectivity can provide a potential entry point for cyber-attacks, which could compromise not just the AR/VR systems but other connected devices in the home as well [80]. The cameras and sensors integral to AR/VR systems, if hacked, could be used to gather detailed information about the home environment and its occupants without their knowledge. The problem of malicious applications is also applicable here.

To mitigate these risks [43,77], it is crucial to develop robust encryption methods for transmitting and storing data collected by AR and VR devices. Secure multi-factor authentication mechanisms that can effectively prevent unauthorized access while maintaining user privacy are also essential. Additionally, privacy-preserving technologies that reduce the amount of data collected, such as processing data locally on devices (edge computing) instead of sending it to the cloud, can help to minimize privacy risks. Additionally, regular security assessments and updates are crucial for maintaining the integrity of AR/VR systems, addressing vulnerabilities promptly and adapting to new threats as they evolve. These controls are designed not only to protect user privacy and security, but also to maintain trust and enhance the overall user experience on AR and VR platforms.

3.3. Physical Home Security and Monitoring

Smart locks, an integral component of the modern smart-home ecosystem, represent a significant shift from traditional mechanical locks to more sophisticated, digitally operated systems [54]. These devices provide users with the ability to lock and unlock doors via smartphones, vocal commands, or even remotely through the Internet. While the convenience and enhanced functionality of smart locks are undeniable, these features also introduce a range of security vulnerabilities that could potentially expose users to risks, such as unauthorized access and data breaches.

The core appeal of smart locks lies in their connectivity, which allows users to control access to their homes from virtually anywhere. This convenience, however, also offers several routes for cyber-attacks [81]. Most smart locks connect to the home's networks via Wi-Fi or Bluetooth, and any weaknesses in these communication protocols can be exploited by hackers to gain control of the locks. For example, flaws in Bluetooth security, such as weak pairing mechanisms or vulnerabilities within the Bluetooth protocol itself, can allow attackers to intercept communications between the smart lock and the user's device to unlock doors without permission.

Furthermore, many smart locks are integrated into broader smart-home systems and managed through home automation platforms that collect and store personal data [82]. This integration can extend the impact of a potential breach, where compromising a smart lock could provide a gateway to access other sensitive systems and information, including surveillance cameras and personal data stored on networked devices. The risk is compounded by the fact that many users often do not change default passwords or fail to implement strong authentication measures, leaving their smart locks—and by extension, their homes—vulnerable to physical intrusion.

Researchers are also exploring the potential of blockchain technology to provide a more secure and decentralized framework for managing access permissions without relying on a central control point that could constitute a single point of failure [83,84].

Moreover, there is an ongoing push towards developing more intelligent threat detection systems that can adaptively recognize and respond to suspicious activities in real time. ML algorithms could play a crucial role in this area, learning from historical data to identify patterns of normal behavior and detect anomalies that could indicate an attempt to manipulate the lock system [85].

Manufacturers of smart locks have taken various measures to mitigate these risks [82], including the use of advanced encryption techniques to secure communications between the lock and its controllers. Many smart locks now feature encryption protocols, such as the Advanced Encryption Standard (AES), which is also used in many other secure communication platforms. Additionally, to counter the risks of unauthorized access, manufacturers have started implementing features such as geofencing, which automatically locks or unlocks doors based on the user's physical location, detected via their smartphone's GPS.

Ultimately, securing smart locks is a complex challenge that requires a multidisciplinary approach. It involves not only advancing the technological defenses, but also promoting user education and awareness about the best security practices [86]. Users must be informed about the importance of using strong and unique passwords, enabling two-factor authentication where available and regularly updating their devices' firmware to protect against the latest threats.

The integration of surveillance cameras into smart homes significantly enhances security, but also exhibits unique challenges and vulnerabilities [55]. These devices, central to home security, are increasingly smart, interconnected, and capable of recording high-resolution video. However, this connectivity exposes them to several unique security threats that need addressing to protect users' privacy and maintain the system's integrity [87].

One of the primary concerns with smart-home surveillance cameras is their susceptibility to hacking. Intruders can gain remote access to these cameras via unsecured networks or through the exploitation of firmware vulnerabilities [9,88]. Once accessed, these cameras can be manipulated and turned off, alter their recordings, or even use them to secretly monitor the activities of the household.

Moreover, these cameras collect vast amount of data, presenting significant privacy concerns [89,90]. If intercepted, video footage can be used maliciously, revealing the personal routines and private moments of individuals. The encryption of data streams and the secure storage of recorded footage are, thus, critical components that need reinforcing across smart-home security systems.

Furthermore, as outlined in the research, advanced methods, like ML algorithms, are increasingly used to differentiate between regular activities and potential security

threats [91]. These systems can identify an intruder even under challenging conditions, such as in cases with low light or when faces are partially obscured. However, these sophisticated features also introduce complexity into the system, potentially leading to false positives or the mishandling of data.

To address these challenges, enhancing the physical security of the camera itself [88], such as through tamper-detection mechanisms, and improving the encryption used during data transmission are vital. Also, manufacturers need to ensure regular firmware updates to protect against the latest threats and implement robust authentication measures to prevent unauthorized access.

Future research should focus on developing more resilient ML models that can accurately detect anomalies while preserving privacy. There is also a growing need for comprehensive frameworks that govern data handling processes, ensuring that user data are protected and only accessible under strict conditions. This holistic approach to security will be essential as smart-home technologies become increasingly integrated and complex.

3.4. Ambient Living Devices

Smart vacuum robots [56], as an integral component of the smart-home environment, have transcended their traditional role to embrace functionalities enriched with IoT capabilities, such as mapping household layouts and scheduled cleaning, operated via smartphone applications. However, as they become more embedded in our personal spaces, the security challenges and vulnerabilities associated with these devices are also magnified.

A primary security concern with smart vacuums is their connectivity to the home's network, which if compromised, can serve as a gateway for attackers to infiltrate other connected devices. This vulnerability is exacerbated by the fact that many smart vacuums operate on common operating systems, like Linux, making them susceptible to known exploits and attacks that can gain root access to the devices. For instance, researchers have demonstrated how vulnerabilities in the vacuum's firmware can be exploited to gain unauthorized control over the device, using it to map private spaces or even operate as a listening device [92].

Another significant risk is related to the data collected by these smart vacuums, which includes detailed maps of users' homes [92]. These data, if intercepted or improperly handled, could pose severe privacy risks. Intriguingly, some research has shown that the lidar sensors on these vacuums can be repurposed to eavesdrop on conversations by interpreting vibrations in objects, highlighting a novel attack vector that turns benign household devices into potential spy tools.

Moreover, the interconnectivity of these devices with cloud-based platforms for enhanced functionality, like remote control and software updates, introduces additional layers of vulnerability. Data transmitted between the vacuum and the cloud, or stored within the cloud, are at risk of interception or exposure unless properly encrypted and managed. The integration with mobile applications further extends the threat landscape, as insecure application development practices can lead to data leaks and unauthorized access to the vacuum's controls.

In response to these vulnerabilities, there is a pressing need for manufacturers to implement robust security measures that address both the physical security of the devices and the integrity of the data they handle. This includes securing communication channels with strong encryption, ensuring secure authentication mechanisms, and providing regular firmware updates to patch known vulnerabilities.

Future research in the security of smart vacuums should focus on developing more sophisticated detection systems to identify and mitigate attacks in real time, enhancing data privacy measures to protect sensitive information, and exploring the use of blockchain and other decentralized technologies to secure device communication and data integrity.

Overall, the proliferation of smart vacuums and similar IoT devices in smart homes presents a complex set of security challenges. It requires multi-faceted strategies to ensure

that the related equipment will not compromise the privacy and security of the environments they are designed to enhance.

Smart-home security is a rapidly evolving field, spurred by the widespread adoption of various interconnected devices that aim to enhance convenience and efficiency in the household. Other examined devices, including smart lighting, thermostats, air-conditioning systems, ovens, fridges, and smart plugs, bring numerous benefits, but also introduce a plethora of security risks that must be addressed to protect homeowners from potential threats.

Starting with smart-lighting systems, these devices offer the ability to control lighting remotely, set schedules, and even adjust lighting based on ambient conditions or occupancy detected by sensors [57]. However, their connectivity to the home network makes them vulnerable to cyber-attacks, where hackers could potentially gain unauthorized access to the network through poorly secured lighting systems. Once accessed, attackers could manipulate lighting settings to disrupt the household or use the system as a gateway to launch further attacks on more critical systems.

Smart thermostats, which adjust the temperature based on user behavior and preferences, present similar risks [58]. These devices collect detailed information about a user's daily routines and home occupancy patterns, making them a rich target for cybercriminals. If compromised, such data can be exploited for burglary or more targeted attacks. Furthermore, unauthorized control over the thermostat can lead to energy waste or damage to the home environment by extreme temperature adjustments.

Air-conditioning systems, increasingly smarter and interconnected, are susceptible to the same threats as smart thermostats [59]. By gaining control over these systems, attackers could cause discomfort or increase utility bills significantly. More dangerously, if integrated with other home-automation systems, compromised air-conditioning units can serve as entry points to other devices connected to the same network.

Smart ovens and fridges represent a more direct physical threat, if compromised [60,61]. A hacked oven could be turned on or off remotely, posing fire risks or other safety hazards. Smart fridges, which often include interfaces to order groceries or manage expiry dates, contain personal consumer data that, if accessed, could lead to privacy breaches. Moreover, since these appliances are central to daily living, their disruption can cause significant inconvenience and potential health risks.

Smart plugs, which are used to control various electronic devices remotely, amplify the security challenges in a smart home [62]. These devices can switch appliances on or off and monitor energy usage, providing convenience and efficiency. However, if compromised, smart plugs could be used to manipulate the power supply of critical devices, such as medical equipment, security systems, or refrigeration units, leading to dire consequences.

To combat these risks, robust security measures are necessary [63,64]. These include strong and unique passwords for device access, encrypted communications to prevent data interception, and regular software updates to patch vulnerabilities. Manufacturers must also prioritize building secure devices that can resist the latest types of cyber-attacks. This involves not only securing the device software and communication channels, but also ensuring physical tamper resistance.

Implementing network segmentation can significantly enhance security by isolating smart-home devices from each other and the main computing environment. This way, even if one device is compromised, the breach does not necessarily grant access to other devices or sensitive personal data stored in other network segments.

3.5. Other Aspects and Actuators

Smart-home security extends beyond the technological vulnerabilities of devices; it encompasses human factors, user awareness, device management, disposal practices, universal standards, and manufacturers' responsibilities [65,66]. Understanding and addressing these aspects are crucial for creating a secure smart-home environment.

The human factor plays a pivotal role in smart-home security [66]. Users often lack awareness of potential security threats and the necessary practices to mitigate them. For instance, many users might not change the default passwords on their smart-home devices, which can make them vulnerable to attacks. Moreover, the convenience of voice-controlled devices can lead to inadvertent disclosures of personal information if conversations are recorded or monitored without user's consent. Users must be educated about the potential risks associated with smart-home devices and trained on the best practices for setting up and maintaining these devices. This includes understanding the importance of securing the home's Wi-Fi networks, recognizing phishing attacks, and knowing how to check and update device security settings in a regular basis. Therefore, enhancing user awareness through education about secure installation, maintenance practices, and the risks associated with careless usage is imperative.

The management and disposal of smart-home devices also present significant security concerns [65]. Proper management involves regular updates and patches of firmware and software, which can protect against known vulnerabilities. However, many users are either unaware of how to update their devices or neglect this critical maintenance step. As for disposal, improperly discarded devices can become sources of data breaches. For example, a smart thermostat or a home-assistant device may retain user data that could be extracted by malicious actors, if not correctly sanitized before disposal. Encouraging responsible disposal practices and providing clear instructions for wiping data can help to mitigate these risks.

Manufacturers play a crucial role in the security of smart-home ecosystems [70,76,82]. Their focus on securing devices should begin at the design phase, integrating strong encryption methods, secure authentication processes, and robust protection against physical tampering. Moreover, manufacturers need to commit to providing ongoing support for their products, including regular security updates and patches. Transparency regarding known vulnerabilities and quick responses to security threats can help to build trust with consumers. Furthermore, manufacturers can contribute to better security practices by making devices that are easier for consumers to manage. Simplifying the user interface for checking and updating security settings, applying enhanced security by default (i.e., enforce multi-factor authentication, regular password updates, etc.), and providing clear, user-friendly instructions for setup and maintenance can greatly enhance the overall security of smart-home systems. Additionally, incorporating features that alert users to potential security threats or needed updates could further protect consumers and their data.

On the regulatory front, the lack of universal security standards for smart-home devices complicates the enforcement of consistent security measures (e.g., [93–98]). Different countries may have varied regulations regarding data protection and device security, making it challenging for manufacturers to comply with all guidelines. Developing comprehensive international standards that address the security requirements of smart-home devices could streamline manufacturers' efforts to enhance security features across markets. Such standards would also aid consumers in making informed decisions about the security of the products they choose to integrate into their homes.

4. Analysis and Discussions of the IoT Setting

4.1. Architectural Structure of IoT Ecosystems

In order to study the security of a smart-home environment deploying IoT technology, one should first describe the architectural structure of such systems. Ordinarily, devices are communicating at the edge system, directly or via a gateway, and can also interact through the Internet or a cloud.

The layers of an IoT architecture are not defined by a single methodology or standard, but rather by a combination of industry best practices, architectural principles, and various standardization bodies. However, several organizations and standardization bodies provide guidance and frameworks for designing and implementing IoT architectures. Some of the most notable ones include the following:

- International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC): The ISO and IEC have developed several standards related to IoT, including ISO/IEC 30141 [93] which provides guidelines for the architecture and interoperability of IoT systems. While the ISO/IEC standards may not explicitly define the layers of an IoT architecture, they offer principles and recommendations for designing scalable and interoperable IoT solutions.
- Institute of Electrical and Electronics Engineers (IEEE): The IEEE has published numerous standards and guidelines for IoT, including IEEE P2413 [94] which defines an architectural framework for IoT. While IEEE P2413 does not prescribe specific layers, it outlines key architectural concepts and considerations for IoT systems.
- Industrial Internet Consortium (IIC): The IIC has developed the Industrial Internet Reference Architecture (IIRA) [95], which provides a comprehensive framework for designing industrial IoT solutions. While focused on industrial applications, the IIRA can be adapted for other IoT use-cases and includes concepts related to layered architectures.
- Open Connectivity Foundation (OCF): The OCF has developed standards for interoperability and connectivity in IoT devices and ecosystems [96]. While the OCF standards primarily focus on interoperability protocols, they also address architectural principles that may align with layered approaches.
- National Institute of Standards and Technology (NIST): The NIST has published several documents related to IoT security and architecture, including the NIST Cybersecurity Framework [97] and NIST Special Publication 800-183 [98], which provide guidance on IoT device cybersecurity. While not explicitly defining layers, these documents offer principles and recommendations for designing secure IoT architectures.

Overall, while there is no single methodology or standard that defines the layers of an IoT architecture, various organizations provide guidance and frameworks that can drive the design and implementation of IoT solutions. Architects and designers often refer to these resources to develop architectures that meet the specific requirements and objectives of their IoT projects.

Nevertheless, based on these methodologies four conceptual levels are considered in IoT research (e.g., [19]):

1. Application: smart environment, smart home, smart city;
2. Perception: movement sensors, smoke sensors, pressure sensors;
3. Network: nodes, servers, topologies;
4. Physical: smart phones, smart appliances, power supplies.

These layers are detailed in the following subsections.

A modern IoT system consists of various smart environments, such as smart homes, cities, hospitals, and transport, all of which are supported by applications that run on smart devices. The application layer [99] is the topmost layer in the IoT architecture and manages all these applications and their secure deployment on user's devices. It is responsible for ensuring the confidentiality, integrity, and availability of legitimate software and its data, as well as that the applications can interconnect and interact with the lower layer, which is the network layer. The network layer is responsible for ensuring the smooth operation of applications and the delivery of services provided by the IoT system. This layer also separates the data collected by different sensors from smart devices for different applications. However, the application layer is highly vulnerable to attacks and intruders who may try to exploit vulnerabilities in the architecture [99].

The perception layer consists of various devices and technologies designed to gather input from the surrounding environment. This includes pressure sensors, smoke sensors, vibration sensors, and RFID sensors. Its primary role is to collect and modestly process information, acting as a component of a larger, intelligent system. Often referred to as the sensing layer, it faces several challenges. Among these, the most critical issue is the efficient collection and capture of data [100].

The network layer [101] is accountable for ensuring that the devices in an IoT system are efficiently connected to each other so that they can communicate, exchanging data through the creation of a communication channel that links the terminal nodes to the servers. This level is essential in both telecommunications and Internet networks since it is responsible for transmitting data to and from the intermediate devices within the system. Its main responsibility is to securely send data collected by sensors to remote nodes, acting as a bridge between the local network and the remote node. Wired or wireless communication is used to connect devices and share necessary data, ultimately providing the desired services through applications managed by the topmost layer, the application layer.

The final layer of the IoT architecture is the physical layer [102], which encompasses the hardware that comprises an intelligent environment with IoT technology. It consists of all smart devices, such as smart phones, computers, tablets, smart watches, smart TV, smart locks, smart smoke detectors, and others, which have sensors to collect data. Additionally, the required hardware for all smart devices to connect to the IoT network, whether wired or wireless, is also included at this level. Hence, it provides the physical connection of the devices as a service to its immediate superior layer, the perception layer.

4.2. Threats Faced by a Smart Home and Related Countermeasures

As the number of Internet-connected devices that support IoT technology grows, there is an increasing need to prioritize security measures in these systems [103]. This is particularly important because these systems are often responsible for securing homes from potential intruders and responding to emergencies, such as fires or smoke detection. In a smart-home system, all smart devices are connected to the Internet via a gateway that serves as the intermediary between the local network and the Internet. However, in order to establish a secure IoT smart-home system, it is crucial to implement robust security protocols at every level of the architecture (see Figure 2).

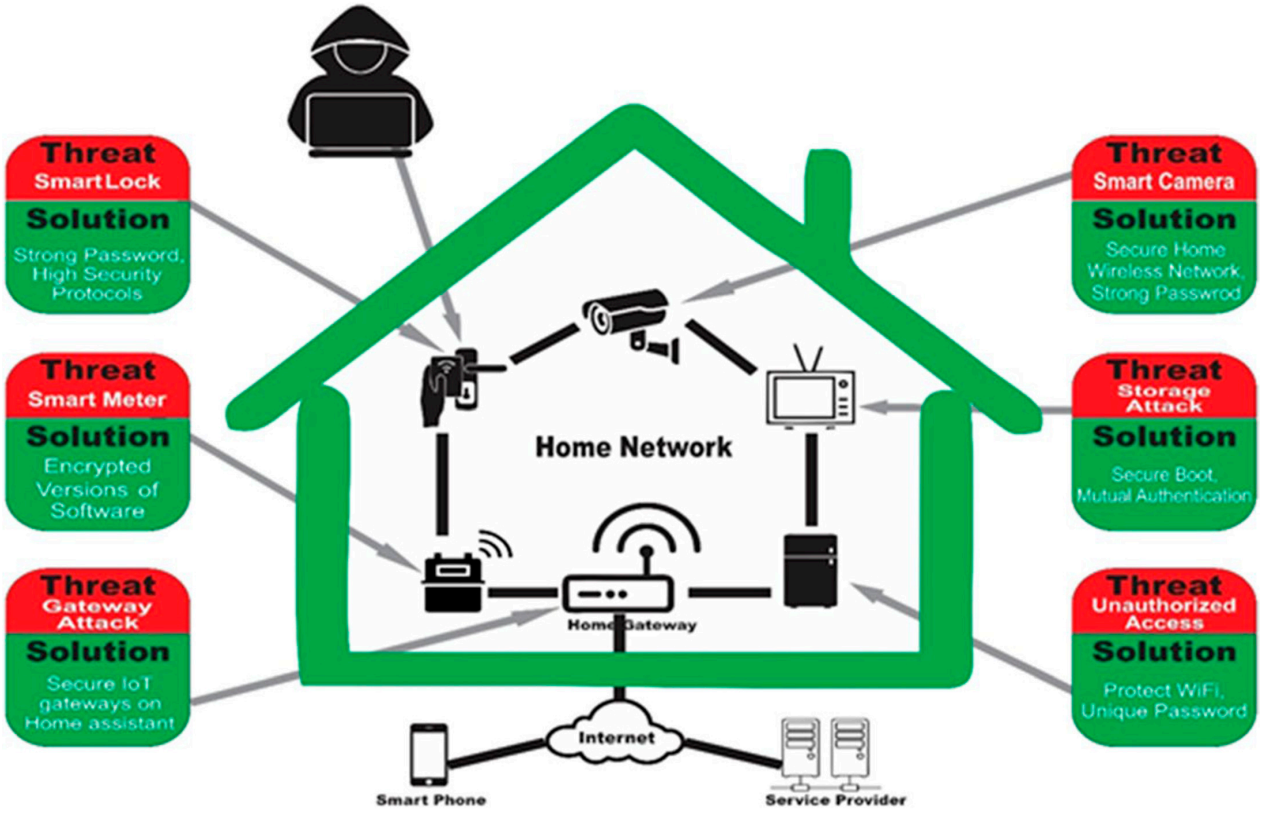

Figure 2. Smart-home threats and countermeasures [30].

Below, we present and analyze the attacks that can be launched on each level separately, as well as the relevant countermeasures and controls that can mitigate them.

4.2.1. Application Layer Analysis

Attacks on an application or set of applications can cause them to malfunction, rendering them unable to perform their intended services. Several types of attacks can be carried out on such systems.

One type of attack is called "social engineering", where the attacker targets the user directly [104,105]. The attacker communicates with the network's legitimate administrator, often applying psychological pressure, to obtain sensitive codes that will allow them to access applications and exploit their services. Sometimes, attackers send disguised emails to deceive users into visiting websites that are replicas of legitimate ones, with the intention of stealing passwords, a tactic known as phishing. This is one of two ways in which the user can fall victim to an attack. The second approach involves the installation of malware that appears user-friendly, with the users being deceived to install the malicious software on their device [103,106,107]. As a result, the attacker gains complete access to the system's data and operations [108,109], including management control. This attack typically targets devices with Internet access and can cause the entire system to crash. Today, phishing attacks are prevalent in Internet-based systems.

Another form of cyber-attack involves sending malicious software to a device [39,110–113], which can either be used for phishing or to cause partial or complete system destruction. Malware, also known as worms, can be found on various websites and can infect devices running different operating systems, such as Linux. Typically, home systems are targeted, specifically their Internet-connected devices, such as cameras and routers, which can result in the collapse of a home's security system. The Mirai botnet attack is such an example, where the attacker monitors the system's activity. Ransomware is another attack where malicious code encrypts the user's data, demanding a ransom to decrypt it. This type of attack affects the last two layers of the IoT architecture and significantly impacts the behavior of the application layer. Also, crypto-jacking attacks of smart-home devices involve unauthorized use of a device's processing power to mine cryptocurrency, often resulting in lower device performance and increased electricity consumption without the user's knowledge.

Another category of attack involves targeting nodes [114–116]. The aim of such attacks is to install harmful software (rootkits) on the system's devices to take control of the applications they oversee. By doing so, the attacker can alter the way the devices respond and behave, resulting in an abnormal, and often unwanted, system performance. The attacker can then impersonate an authorized user by deceiving the system, causing serious security implications.

When an attacker tries to trick the system and pretend to be an authenticated user, it is considered an access control attack. This type of malicious activity targets the involved nodes of the system and can result in serious security consequences [13,117,118].

Unlike computers, a system's smart-devices do not automatically update/upgrade their security software [119–121]. When updating the security software on one device, there is a parallel distribution of a copy of the software to the rest of the devices in the system, with the result that for as long as this update lasts, the system is out of order. Therefore, during this time, no encryption might be required, and thus, there is an open opportunity window for attackers [122].

Unauthorized software installation from untrustworthy developers, who often disregard security protocols and standards, can create vulnerabilities that attackers can exploit to breach the security of devices [123,124]. In the IoT realm, many devices have default settings and an operating system that lacks authentication requirements. As a result, attackers can easily gain access and modify these settings at will. Smart homes and IoT environments rely on remote communication with servers that store and manage large amounts of data to support the services required by the applications. However, this type of communication

raises significant security concerns, leading to various issues related to system security and the quality of service at the application layer.

The application layer can also be susceptible to attacks, involving the unauthorized reconfiguration of remote devices through the Internet [11,12,125]. If devices lack proper software protection and strong security protocols, potential attackers may attempt to reconfigure network devices and change their settings to their own preferences, allowing them to gain access to sensitive personal information transmitted between devices on the network.

This level is responsible for the correct and smooth operation of the applications hosted by the devices, in order to provide the electronic services. To be able to deal with phishing attacks, users, either as administrators of the home environment or the server, should be trained in order not to be misled by fake emails or fake websites. But also, proper user authentication at the network level can prevent a phishing attack [15,108]. Abbas et al. [126] propose a threat modeling approach specifically designed for IoT and smart-home use-cases to identify and mitigate social engineering and phishing threats effectively. The method uses the STRIDE threat modeling approach to systematically identify potential threats that could lead to phishing attacks. By implementing this approach, IoT researchers, engineers, and cybersecurity policymakers can enhance security measures during the early design stages of IoT systems, ensuring more secure deployments in critical infrastructures. Technically, there are several studies that are trying to utilize ML for the detection of phishing messages [127–130]. Then, these solutions can be integrated by the system developers to classify automatically received messages and block malicious attempts before reaching the user. Nevertheless, raising the user's awareness (e.g., training, informative campaigns, etc.) for these threats is one of the main controls that are recommended [16,17].

One way to detect the presence of malicious code or malicious applications in application stores is by following a strategy which measures the normal execution time of the processes that the nodes execute in "normal" conditions. When in other measurements this time exceeds the usual, it means that the node additionally employs unwanted, extraneous, and malicious software [35,111]. Ficco [131] proposes an innovative method for detecting malware in IoT devices by utilizing Markov chain behavioral models to analyze the sequence of API calls made by applications during execution. This dynamic analysis approach creates a behavioral model of the applications, represented as a Markov chain, where transitions between states (API calls) help to distinguish between benign and malicious applications, based on their unique patterns of API usage. Sharmeen et al. [132] focus on enhancing the detection of malware threats in industrial mobile-IoT networks through a comprehensive analysis of different detection techniques, specifically static, dynamic, and hybrid approaches. The authors present a detailed performance comparison of these methods, focusing on aspects like data set characteristics, feature extraction, selection techniques, and achieved accuracy. By analyzing and identifying suspicious API calls, system calls, and permissions, this solution aims to assist application developers in creating safer applications for IoT settings. The main solution proposed by Wang et al. [133] is the development of a novel methodology to construct and evaluate features for detecting malicious applications in Android. This approach involves a comprehensive taxonomy of features derived from static, dynamic, and meta-data analyses. This solution emphasizes the importance of accurately defining and extracting these features to improve the performance of ML algorithms in distinguishing between benign and malicious applications.

Apart from authentication mechanisms that are designed to utilize the features of modern smart-home devices (e.g., authentication for AR/VR glasses [78,79]), researchers are proposing general authentication and authorization solutions for the smart-home setting. For example, Nimmy et al. [134] propose a novel multi-factor authentication protocol specifically designed for smart-home environments, utilizing Elliptic Curve Cryptography (ECC), secret sharing, and Photo Response Non-Uniformity (PRNU) to enhance security. The protocol aims to uniquely identify user smartphones and ensure mutual authentication among all entities involved, making it resilient to common attacks, such as smartphone

capture. Additionally, it leverages face biometrics to authenticate users, ensuring both the security of transactions and ease of use without the need for passwords or smart cards. In another work, Nimmy et al. [135] define a novel, lightweight, and privacy-preserving remote user authentication protocol. This protocol leverages geometric secret sharing and PRNU to establish mutual authentication among users, their smartphones, and IoT devices without the need for passwords or smart cards. It ensures robust security against common attacks, such as phishing and smartphone capture, and its lightweight nature makes it suitable for deployment on heterogeneous and resource-constrained IoT devices.

Nagy et al. [136] introduce a sophisticated approach to rootkit detection for embedded IoT devices by utilizing a TEE. This method capitalizes on the TEE's ability to provide an isolated operating context, which prevents rootkits, even those with root privileges, from interfering with the detection process. The solution involves identifying anomalous modifications made by rootkits to the OS kernel code, system programs, and control flow data, as well as detecting rootkit components in persistent storage.

Haney and Furman conducted a series of studies concerning the subject of updates' management for smart-home devices. The initial study focused on exploring smart-home users' perceptions and experiences with device updates, particularly in terms of security [137]. The researchers found that many users do not associate updates with security enhancements and often overlook or delay installing them. The paper proposed a follow-up survey aimed at a broader audience to delve deeper into these perceptions and enhance our understanding, which could lead to the development of more effective, user-friendly update mechanisms and communications that emphasize the security benefits of timely updates. In their next study [138], the solution proposed focused on expanding user education and awareness, improving the transparency of update purposes and processes, and enhancing the usability of update mechanisms to ensure that users can easily and promptly apply necessary updates to their smart-home devices.

4.2.2. Perception Layer Analysis

A favorite tactic for attackers is attacking at the level of perception. As mentioned above in this paper, at the perception layer, all devices communicate, collect, and exchange data, using the sensors that each one of them possesses. In this case, the attacker tries to intercept and modify the communication software of the networking nodes, so that a device of his/her own can enter and be accepted in the network, now also receiving the sensitive information that is trafficked towards it. All devices communicate with a remote server (e.g., cloud) via the Internet. This communication is performed automatically and without particularly strong security protocols, which makes it vulnerable to third-party attacks. Thus, a device external to the network can intervene in this communication and intercept the data that the networking devices have collected and intend to send to a remote server for further processing. This attack is also known as eavesdropping [139,140].

An alternative attack path for attackers to disable and remove sensors or devices from the network is by installing a sniffer application on them and reactivating them. They gain access through this application to the data managed by the sensors [141].

Another vulnerable point in the network is when the devices need to be restarted. Then, the system in preparation does not have time to "run" the security software and security protocols, such as UART or JTAG. At this moment, attackers can attack the system. These attacks are also called boot attacks [22,117].

Most devices in a home environment often operate with low power consumption. This makes them vulnerable to attackers, who, after disabling them, can replace them with their own, "fooling" the network and collecting the sensitive information being trafficked towards them [141]. An attacker can even reprogram a certified device by checking its sensor, collecting all its data.

Another way to intercept data is with side-channel attacks [117,142]. These attacks are usually timing attacks, electromagnetic attacks, and laser attacks. These attacks create a parallel side channel, which steals, "eavesdrops" on the information exchanged by the

devices' sensors in a network. This is feasible due to the low power, communication mode, and architecture followed by the sensors in an IoT system.

The wireless connection and remote communication of many devices in one IoT system is carried out with the existence of noise. Noise is incomplete false irrelevant information—information, however, that may come from intruders and that can cause problems in the network [143,144]. Noise causes the sensors to malfunction, causing them to misbehave and transmit incorrect data to end-nodes, which is a major problem for the system's security [117,145].

The first interaction point of the system is its sensors. Sensors must be equipped with appropriate security measures in order to become resistant to attacks. Otherwise, they should not be exposed to third parties and should be kept in a safe place.

At this level, the sensors are the target of attacks. Thus, the proposed solutions involve protecting the data collected and exchanged between the sensors. To mitigate the relevant attacks, various sensor interconnection and operation models are proposed, covering sniffing, path loss, shadow fading, and Rayleigh fading detection. Firstly, to protect the system from eavesdropping and sniffing, the system should run on a private and not on a public and free network, where an attacker may have easy access. On many occasions, attackers create private networks with names of public entities in order to trick users into connecting to them. Also, a device integrated in an IoT system should operate with encrypted code techniques. The device should run software from a trusted and certified developer and work with Original Equipment Manufacturer (OEM) hardware. Therefore, by using secure equipment from certified manufacturers, either at the hardware level or at the software level, the chances of successful attacks are minimized. Nevertheless, in the presence of an attacker, several methods are suggested to avoid eavesdropping and sniffing. Abrishamchi et al. [146] propose a hybrid energy-efficient privacy-preserving scheme designed to enhance privacy in smart-home environments by effectively countering wireless traffic snooping. This scheme utilizes a probability-based decision-making algorithm to control the injection of dummy packets and adjust transmission times, thereby maximizing the confusion for attackers trying to decipher the network traffic patterns. By blending energy efficiency with robust privacy protection, this approach aims to secure smart-home communications against eavesdropping without causing significant delays or excessive energy consumption. Mechanisms that leverage AI and neural networks contribute significantly to defense against side-channel and noise attacks. Xinchuan and Martinez [147] utilize a neural network, which through continuous measurements can learn what is the desired, "smooth" operation of the system, easily identifying cases where noise has entered the system (anomalies). Also, in order not to leak the sensitive information of the system, Zhihua et al. [148] proposed a Public Key Infrastructure (PKI) solution where information is encrypted with a public key algorithm, such as the leakage resilient algorithm, in order to ensure confidentiality even in the case of loss of some bits from transmitted packets. Moreover, to counter booting attacks, Yuan et al. [149] suggest a secure boot process of encrypting the FPGA-bitstream to protect the IoT device from bitstream decoding, encrypting the system boot image to enhance system security, and ensuring that the device operates correctly, as intended, via authentication.

4.2.3. Network Layer Analysis

The network layer is responsible for the correct pairing of devices with each other and subsequently for their correct communication. At this level, the required authentication of the devices involved in the network takes place, but this level is also vulnerable to attacks. One form of attack involves the sending of a large amount of data that the system is unable to process. This overflow of data causes congestion in the nodes, and as a result, they cannot respond to even the simplest functions. This attack is called a Denial of Service (DoS), and when it happens, it blocks even the legitimate and authorized user from accessing the network [124,150]. Thus, the attacker finds an opportunity to enter the network and modify the pairing parameters of the devices, receiving all information.

Another form of attack is the gateway attack, where the attacker modifies the routing process between smart devices, resulting in information being sent through another route that leads to the compromised devices. The gateway attack aims to collapse the connection between the sensors and the remote server of an Internet Service Provider (ISP) [145,151,152], an attack which often results in a DoS.

An attack that leads to an unauthorized user accessing the network can cause major problems, as valuable information can be intercepted or even modified to serve the attackers' interests [19,153–155]. Such an attack would be devastating in a smart-health environment, which manages sensitive patient information often with disastrous consequences for the patients themselves. Storing large amounts of personal data on local devices, or even worse on remote servers (cloud), provides poles of attraction for potential attackers, especially when many users have the right to access these data [156–158]. This is an entry point of the system, where the attacker can pretend to be another authorized user and gain access to the stored and completely private data.

Another popular attack is when the attacker interferes between the communication of the devices by compromising a network device. Thus, without disrupting the operation of the system, it receives all information circulating in the system, an attack also known as a black-hole attack (e.g., in RPL) [32]. A similar attack is that of man-in-the-middle, where communication between nodes is disrupted through a malicious device, creating a large amount of irrelevant data on them and causing confusion in their operation, making the network particularly vulnerable to several security issues [159,160].

Another routing attack is that of flooding with HELLO messages [38]. The attacker bombards a network node with a large number of HELLO messages, claiming to be a neighboring node. The node accepts it as its neighbor and starts communication with it. Due to the high frequency of HELLO messages, the attacking node is treated by the rest nodes as a parent node, and they start sending all the data to it, thus changing the network routing.

The different technologies of sending data between the devices that can be found in a smart environment create many vulnerabilities in the system [143,160,161]. The wide variety of different technologies used in the connections between the devices and the end-node creates many weak points in terms of security [117].

DoS is generally a main concern for computer networks. In ordinary cases where a computer is being attacked by a network of compromised nodes (botnet) through the Internet, ISPs are applying solutions to detect DoS and block the traffic before reaching the target. The defending machine could also deploy anti-DoS mechanisms for networks or services, like backoff algorithms. Hatzivasilis et al. [162] propose WARDOG, an end-user awareness system designed to mitigate botnet infections on host devices. It operates by alerting and enabling infected machines to automatically block malicious activity once a botnet attack is detected, primarily focusing on DDoS attacks. The system not only informs the end-user of the infection, but also gathers and processes forensic data to legally document and potentially prosecute the attackers. Key features of WARDOG include its compatibility with the existing Internet infrastructure, transparency to the end-user, scalability across many users, and the ability to handle various types of malicious activities without economic impact to ISPs or end-users.

To safeguard applications that allow unauthorized access, as well as to counter man-in-the-middle attacks, Alizal et al. [163] developed a secure and efficient multi-factor device authentication scheme. The proposed scheme uses digital signatures and device capability to authenticate a device. Thereupon, a device will only be allowed into the network if it is successfully authenticated through multi-factor authentication; otherwise, the authentication process fails and the whole authentication process restarts. The scheme not only authenticates the device very efficiently through multi-factor authentication, but also authenticates the authentication server with the use of digital signatures.

After proper authentication, role- or attribute-based authorization can be enforced. Ameer et al. [164] argue that attribute-based control policies are better suited for smart-home

applications. Therefore, they propose a related solution, called HABACα, an attribute-based access control model tailored for smart-home IoT environments. This model is dynamic and fine-grained, capturing various characteristics of users, environments, operations, and devices to construct comprehensive access control policies. HABACα enhances traditional models by incorporating attribute-based mechanisms that adapt more flexibly to the changing conditions and complex requirements of typical smart-home setups.

In order to protect the network against routing and forwarding attacks (e.g., flooding), Hatzivasilis et al. [165] introduce SCOTRES, a secure routing system designed for IoT and cyber–physical systems (CPSs) in wireless networks. SCOTRES is a trust-based system that utilizes five innovative metrics to enhance network security and performance: energy, topology, channel health, reputation, and trust metrics. This system seeks to intelligently distribute network loads, increase the lifetime of the network, provide robustness against jamming attacks, and ensure cooperative behavior among nodes.

Moreover, IDS/IPS solutions are required to monitor the system and counter a series of problematic conditions. Usually, their core algorithm is based on pattern matching or ML for attack identification or anomaly detection. Rajora and Sharma implement an IDS/IPS for the smart-home IoT devices [166]. They propose TWINKLE, an innovative architecture designed for IoT-enabled smart homes, focusing on enhancing intrusion detection and prevention within such networks. TWINKLE operates in two modes: a normal mode—which conserves resources; and a watchful mode—which is activated when suspicious activity is detected. This approach allows for a dynamic and efficient use of resources, minimizing overhead while enhancing the detection and mitigation of cyber threats like DDoS and sinkhole attacks. Through case studies, TWINKLE demonstrates significant improvements in reducing detection delay and resource consumption compared to existing systems, positioning it as a viable solution for resource-constrained environments.

4.2.4. Physical Layer Analysis

The installation of an electric power supply in smart devices is a building block of the IoT system. Power failure is a factor that makes the system particularly vulnerable [167,168]. There should be a mechanism that can protect the devices and the system from a power outage, which can be caused either due to extreme weather phenomena or due to the intervention of a third party to create fertile ground for attacks. An environmental attack is considered an attack that a device experiences due to a weather phenomenon [169,170]. For example, a sensor can be damaged when exposed to heavy rain or falling snow. This may lead to its malfunction and consequently affect the efficiency of the entire system, causing many problems. Smart devices, most of the time, operate with a specific supply of electrical power, without the possibility of backup energy sources in case of exhaustion or interruption of the central supply. When these devices run out of power, they automatically go into low-power mode. This results in their limited operation, making them unable to meet 100% of the system's needs or sending incorrect information [171,172]. These are hardware failures, leading to network and system failures, and it only takes one device to be underpowered due to low power for this to happen.

A sensitive part of the system is the wireless connections between its devices, where they are targeted by attackers who bombard them with radio signals, known as jamming, in order to interfere with their communication. This can lead to total or partial network collapse, depending on signal strength [173]. However, even in the partial malfunction of the network, in order for the affected nodes to do the required filtering, they lose a large percentage of their power, since they are forced to transmit the data when they regain communication, causing many side-effects, as described above.

Also, another attack is to inject malware through the debugging interface [169]. A malicious device can spoof the network by pretending to be an authenticated device and spread the malware to all nodes, thereby enabling a third party to intercept sensitive information or even shut down the entire system.

One type of attack on the physical layer is a bombardment of the network with noise signals, i.e., unnecessary and useless information, interfering with the operation of the Radio Frequency Identification (RFID) part. The RFID is underpowered and cannot send information to the devices with the required power [33]. Finally, another attack on this layer is the creation of a clone device, with the same characteristics as a certified device, such as the manufacturer, software, and configurations, in order to trick the system, deceiving the RFID counterpart and copying the tags [174,175]. The clone device, after entering the network, spreads malicious software to all nodes in the network, with the aim of intercepting or destroying it. The attacker aims to understand the security protocols and try to copy the tags [30], writing and sending data that will modify the behavior of the system [103,106,107].

The physical layer consists of the system hardware (i.e., the smart devices), but also the devices and components used to interface with each other and with the Internet. A vulnerable point on the physical level is the electricity supply mechanism, where during a power outage which can also be due to extreme weather conditions, the devices are deactivated and a huge hole in the system's security is created. Also, when devices run out of power, they go into low-power mode and start underperforming. Smart devices are vulnerable to attacks, as described above, before and when they are under conditions of extreme weather phenomena. A solution to this includes the deployment of devices in places that will not expose them to those natural phenomena.

Cloning system devices by cloning RFID tags is also a popular attack method. A proposed solution is to hash double collisions with a vector of exact metrics. The double-collision function is used in identifying and determining the flow of tags, where the collection of duplicate hashes and duplicate tag identification detection takes place. Maninder and Sheetal Kalra [140] focused on enhancing the security through a Quantum Key Distribution (QKD) authentication scheme. This scheme aims to provide mutual authentication between users and servers, while ensuring the security of the communication against various cyber threats, including eavesdropping. The implementation uses quantum properties to generate and distribute cryptographic keys securely, leveraging the inherent security features of quantum mechanics to prevent unauthorized access and data breaches, as well as harden the cloning of devices.

Jamming is the main concern of wireless communications in the physical layer. Jeyaselvi et al. [176] focused on using the Support Vector Machine (SVM) method to detect cloning and jamming attacks in IoT sensor networks. The system utilizes SVM to classify nodes as either cloned or normal, based on the distance measurements from IoT devices to a base station, enhancing the security and integrity of the network. The approach includes the monitoring of a selected node based on the probability distribution of sensor nodes, which helps in accurately identifying and mitigating clone attacks, ensuring a robust network performance against malicious activities. Mbarek et al. [177] suggested an advanced trust-based authentication scheme for RFID systems, designed to address vulnerabilities, such as jamming and cloning attacks. This solution, named TRAS, incorporates trust factors, like previous keys, transactions history, and node capabilities, into the authentication process, allowing for dynamic and secure verification of RFID tags. This method aims to improve the resilience of smart-home systems against these specific types of security threats by enhancing the reliability and transparency of the authentication process.

4.2.5. Summary of Threats and Countermeasures

Table 1 summarizes the cyber threats for each IoT layer along with the indicative solutions and countermeasures.

Table 1. Summary of threats and examples of countermeasures per IoT layer.

Layer	Threats	Countermeasures
Application	Social-engineering and phishing	Threat modeling [126], ML detection [127,130], user training, and raising awareness [16,17]
	Installation of malicious software and applications	Code and application analysis [131–133]
	Attacks on access control	Multi-factor authentication [134], privacy preserving authentication [135]
	Rootkit attacks	Rootkit detection with TEE [136]
	Failure to install security patches and updates	User education [138]
Perception	Eavesdropping and sniffing attacks	Operate within private networks and transmission of fake packets protocol [146]
	Side-channel attacks	Encrypted communication [148]
	Noise in data	AI and neural network anomaly detection [147]
	Booting attacks	Secure booting with encryption and authentication [149]
Network	DoS	WARDOG device notification and mitigation mechanism [162]
	Man-in-the-middle	Multi-factor authentication of device and server [163]
	Unauthorized access	Attribute-based access control with HABACα [164]
	Routing and forwarding attacks	Trust-based computing with SCOTRES [165]
	Traffic analysis	IDS/IPS [166]
Physical	Loss of power and environmental threats	N/A
	Cloning	Quantum key distribution [140]
	Jamming	ML with SVM classifiers [176], trust-based authentication with TRAS [177]

5. Best-Practices Guide for a Secure Smart Home

Setting up a smart-home device involves careful planning and execution to ensure seamless integration, optimal performance, and security. Here is a best-practices guide to help you set up your smart home devices effectively:

1. Plan Your Smart Home Layout
    1. Identify Needs: Determine what you want your smart-home devices to accomplish. This could range from enhancing security to improve energy-efficiency or simply adding convenience to your daily routines.
    2. Select Compatible Devices: Choose devices that are compatible with each other and can be easily integrated into a single ecosystem. Look for devices that support common standards or platforms (e.g., Apple HomeKit, Google Home, Amazon Alexa).
2. Secure Your Devices
    1. Update/Upgrade Regularly: Set a process to automatically or periodically seek for and install updates/upgrades. Both for firmware and application software.
    2. Disposal Policy: Set safe disposal strategies for all equipment, including secure deletion/destruction of data and even physical destruction of digital components and memories/storage.
    3. Device's Security Controls: Set all potential defenses that are provided by the main manufacturer (e.g., pins, extra security code, networking safeguards, etc.).
    4. Minimize Exposure: Restrict connectivity to the least open/public LANs and networks that are necessary. Minimize the exposure of the system.

5. Set User Privileges: Restrict the number of authorized users to the minimum required. For each user, restrict access rights to the least privileges required.
6. Security Software: Set anti-virus, anti-malware, host-firewall, and host-IDS where applicable.
7. Delete Unnecessary Elements: Remove services, applications, or other elements that are insecure or not in use by the current system (e.g., Telnet).
8. Avoid Outdated Equipment: Do not use outdated devices that are not supported by the vendor anymore.
9. Configure Before Deployment: Before incorporating a new device to your system, verify that it is updated/upgraded, and all security and configurations are properly set.

3. Secure Applications and Software
    1. Use Only Secure Versions: Install the latest secure and stable versions.
    2. Set And Update Before Use: Upon installation, proceed immediately with the proper updates/upgrades, configurations, and settings of security/privacy.
    3. Automate Updates: Set automated or periodic updates/upgrades.
    4. Strong Authentication: Use strong passwords, as well as multi-factor authentication, wherever possible.
    5. Application-Level Protections: Enable application-level firewalls, IDS, extra pins, or other defenses, wherever possible.
    6. Restrict Access: Restrict access rights/permissions and connectivity to the minimum required.
    7. Restrict Users: If applicable, restrict the number of users to the minimum required.
    8. Use Official and Well-Reputed Vendors: Use only official and authenticated applications/software.
        1. Especially for the technicians/engineers, always check the validity of the elements that are about to be installed (e.g., check the digital certification of the website, as well as the digest of the downloaded software).
        2. For elements of unknown or less popular vendors, also check for recommendations from other users in related forums.
        3. Do not install less trusted applications/software in the core of the system, especially if you have not tested them in a less critical part of your setting.
    9. Monitor Operation: Where applicable, install security software for monitoring of the runtime environment and alerting.
    10. Set Build-In Security and Privacy Controls: Check the offered options and set the privacy policies to the minimum required.
    11. Secure Deletion: Apply secure removal strategies, logging out from all accounts and applications, revoking all acquired accesses/permissions, and securely erasing all permanent and temporary data.
    12. Respond to Incidents: Set a response strategy, including details of whom you have to call and your first actions in case you notice something strange. For example, if you start receiving unknown notifications of purchase attempts in your mobile banking, you block your cards immediately and call your bank's 24/7 security service.
    13. Recover from Incidents: Set a recovery strategy in case something happens.
4. Secure All Networks' Networking Devices
    1. Security Configuration: Set the highest possible protections and set as a high priority the protection of the equipment that facilitates networking, especially for the devices that have direct access/exposure to Internet, and especially the main router.
    2. Security Primitives: Activate or set additional firewalls and IDS/IPS. Use the most restrict policies possible.

3. Usage Zones: Create different LANs and virtual LANs (VLANs) for different usage zones of the smart home.
4. Remote Access: Consider setting an in-house virtual private network (VPN) for accessing the smart home remotely (e.g., the surveillance system).
5. Least Privileges: Restrict the privileges of services that are exposed to the Internet.
6. Network Monitoring: Install monitoring systems and periodically audit the activity of your system.
7. Decrease Attack Surface: Disable insecure communication protocols and services (e.g., http), as well as elements that are not currently in use.
8. Regular Updates: Similar with the devices, do not use outdated equipment.

5. Pay Specific Attention to Securing your Wi-Fi Network
    1. Strong Passwords: Use strong, unique passwords for your Wi-Fi network and each of your smart-home devices.
    2. Network Segmentation: Consider creating a separate Wi-Fi network for your smart devices to isolate them from the network you use for personal computing, reducing the risk of cross-device hacking.
    3. Regular Updates: Keep your router's firmware and your smart devices' software up to date to protect against known vulnerabilities.
6. Install and Position your Devices Strategically
    1. Follow Installation Guides: Carefully read and follow the installation instructions provided with your devices. This may include downloading an application, connecting to Wi-Fi, or performing initial setup steps.
    2. Optimal Placement: Place devices in locations where they can function effectively (e.g., smart cameras with a clear field of view, smart thermostats away from direct sunlight).
7. Integrate Devices with a Central Hub or Application
    1. Choose a Central Control System: Select a central hub or application that can control all your devices. This unifies control and makes managing your devices more convenient.
    2. Customize Settings: Adjust settings for each device according to your preferences. This may involve setting schedules, creating automation rules, or defining scenes.
8. Test and Troubleshoot
    1. Test Operations: After setting up, test your devices individually and the system as a whole to ensure they work as expected.
    2. Troubleshoot Issues: If a device is not working correctly, consult the troubleshooting section of the device manual or contact customer support.
9. Educate Household Members
    1. User Training: Educate all household members on how to use the smart devices, emphasizing the importance of security practices, like not sharing passwords.
    2. Manage Your Passwords and Accounts: Consider utilizing password/account managers.
    3. Backup Your Data: Set a backup strategy.
10. Monitor and Adjust
    1. Regular Reviews: Regularly review your smart-home setup to ensure it continues to meet your needs. Adjust settings, add new devices, or remove unnecessary ones as needed.

By following these best practices, you can create a smart-home setup that enhances convenience, efficiency, and security, while also being prepared to adapt to new technologies and needs over time.

6. Directions for Future Research

Combining all the previously mentioned areas, there is a unified list of topics for future research and development in smart-home security across various devices and use-cases that highlight critical avenues for exploration and innovation in this field:

- Enhanced Biometric Security: Developing more sophisticated biometric authentication methods that leverage the unique capabilities of smart-home devices.
- Context-Aware Security Protocols: Creating security protocols that adapt to the user's context and environment within the smart home.
- Decentralized Security Mechanisms: Exploring blockchain and other decentralized technologies for managing identity verification and ensuring data integrity.
- Privacy-Enhancing Techniques: Developing methods for protecting personal data captured by smart-home devices, using advanced anonymization techniques and local data processing.
- Secure Multi-User Interactions: Enhancing security for environments where multiple users interact with the same devices, like smart TV or AR/VR equipment.
- Robust Malware Detection: Implementing sophisticated systems for detecting malware in IoT devices, including smart locks and cameras.
- Physical and Network Security Integration: Investigating ways to integrate physical security measures with network security protocols across smart-home devices.
- Energy-Efficient Security Protocols: Creating security solutions that minimize energy consumption, particularly for devices like smart locks and smart plugs.
- Secure Device Management and Disposal: Ensuring secure lifecycle management of smart-home devices, from installation to disposal, to prevent data leaks.
- International Security Standards for IoT: Developing and promoting the adoption of global security standards for IoT devices to ensure consistent security practices.
- Anomaly Detection Using AI: Leveraging AI to detect and respond to unusual behavior or threats in smart-home environments.
- IoT Device Interoperability and Security: Ensuring that all interconnected smart-home devices adhere to strict security protocols to prevent vulnerabilities.
- Ethical Design and User Consent: Examining ethical issues in smart-home technology deployment, especially regarding surveillance and data-collection practices.
- Forensic Capabilities for IoT Security: Developing forensic tools and techniques for investigating and mitigating security incidents in smart homes.
- Consumer Awareness and Education: Enhancing user understanding of the potential risks and security practices associated with smart-home technologies.
- Regulatory Compliance and Privacy Laws: Addressing compliance with existing and emerging privacy laws and regulations that affect smart-home technologies.
- Advanced Encryption Methods: Researching more robust encryption techniques to secure data transmission between smart-home devices and external networks.
- Hybrid Energy-Efficient Privacy Preserving Schemes: Developing privacy-preserving protocols that balance energy efficiency with effective privacy protection, especially in communication-heavy IoT environments, like smart homes.

This unified list encompasses a broad spectrum of critical research topics that address the complex security and privacy challenges that smart-home environments are facing today. Each topic not only highlights specific technological needs, but also considers broader social, ethical, and regulatory aspects that are crucial for the safe and trusted integration of smart technologies into everyday living spaces.

As smart homes become increasingly interconnected with the proliferation of IoT devices—ranging from smart locks and surveillance cameras to lighting systems and vacuum cleaners—the potential vulnerabilities and privacy concerns these devices introduce cannot be understated. The security risks associated with these devices include unauthorized access, data interception, and the exploitation of network vulnerabilities, which could lead to severe consequences for users' safety and privacy. Throughout this research, we have identified several critical areas that require robust security measures. For instance,

enhanced biometric security, decentralized security mechanisms, and advanced encryption methods are paramount for protecting sensitive user data and ensuring secure communication between devices. Moreover, context-aware security protocols and anomaly detection using AI underscore the need for dynamic and intelligent security systems capable of adapting to new threats as they emerge. The survey also highlighted the significance of addressing not only the technical aspects of security, but also the human factors, such as consumer awareness and education. Ensuring that users are informed and equipped to manage their smart-home devices securely is essential for mitigating risks. Furthermore, the proper management and disposal of smart-home devices play a critical role in maintaining security throughout the device lifecycle. The research directions identified in this survey emphasize the development of privacy-enhancing techniques, secure multi-user interactions, and the integration of physical security measures with network security protocols. These areas represent fertile ground for future studies aimed at enhancing the robustness and user-friendliness of smart-home security systems. Looking ahead, there is a clear necessity for the development of global security standards for IoT devices to harmonize security practices and ensure a consistent level of protection across all smart-home devices. Additionally, exploring the potential of blockchain technology for decentralized security solutions and developing energy-efficient security protocols will be crucial for advancing the field.

In conclusion, as smart-home technologies continue to integrate deeper into the fabric of daily living, addressing the complex security and privacy challenges presented in this survey will be critical. By fostering innovation in both technology and policy and ensuring that security measures keep pace with technological advancements, we can better protect smart-home environments against emerging threats. This survey lays the groundwork for future research and development efforts that will enhance the security, privacy, and usability of smart-home technologies, ensuring a safer and more secure future for users worldwide.

7. Conclusions

In conclusion, this survey on smart-home security has highlighted the extensive security and privacy challenges inherent in the expanding landscape of smart-home technologies. As smart homes grow more interconnected with the increase in IoT devices, the vulnerabilities and privacy issues these devices present are significant. These risks include unauthorized access, data interception, and network vulnerabilities, potentially endangering user safety and privacy. The survey underscores the necessity for robust security measures, like enhanced biometric security, decentralized mechanisms, advanced encryption, and AI-driven anomaly detection, which are critical for safeguarding sensitive data and ensuring secure device communication. Additionally, it stresses the importance of human factors, such as consumer awareness and proper device management and disposal, which are vital for mitigating risks effectively. Future research should focus on developing privacy-enhancing technologies, improving multi-user interactions, and integrating physical with network security. The establishment of global security standards and exploration of technologies for decentralized solutions, like blockchain, are also crucial for advancing the field. Addressing these challenges is essential for protecting smart-home environments and ensuring their safe integration into our daily lives, laying a foundation for future security and privacy enhancements in smart-home technologies.

Author Contributions: Conceptualization, G.V. and E.K.; methodology, N.P.; validation, N.P.; investigation, G.V. and G.H.; writing—original draft preparation, G.V., E.K. and G.H.; writing—review and editing, G.H.; supervision, G.H. and N.P.; funding acquisition, G.H. All authors have read and agreed to the published version of the manuscript.

Funding: This work has received funding from the European Union's Horizon 2020 research and innovation programmes under grant agreements No. 101021659 (SENTINEL) and No. 101070599 (SecOPERA).

Data Availability Statement: Data derived from public domain resources. All related works are referred to the References Section.

Acknowledgments: We acknowledge the funding from the European Union's Horizon 2020 research and innovation programmes.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Ndaguba, E.; Cilliers, J.; Ghosh, S.; Herath, S.; Mussi, E.T. Operability of Smart Spaces in Urban Environments: A Systematic Review on Enhancing Functionality and User Experience. *Sensors* **2023**, *23*, 6938. [CrossRef] [PubMed]
2. Itair, M.; Shahrour, I.; Hijazi, I. The Use of the Smart Technology for Creating an Inclusive Urban Public Space. *Smart Cities* **2023**, *6*, 2484–2498. [CrossRef]
3. Rani, S.; Chauhan, M.; Kataria, A.; Khang, A. IoT equipped intelligent distributed framework for smart healthcare systems. In *Towards the Integration of IoT, Cloud and Big Data*; Springer: Singapore, 2023; Volume 137, pp. 97–114.
4. Kapucu, N.; Bilim, M. Internet of Things for smart homes and smart cities. In *Smart Grid 3.0*; Springer: Cham, Germany, 2023; pp. 331–356.
5. Umair, M.; Cheema, M.A.; Afzal, B.; Shah, G. Energy management of smart homes over fog-based IoT architecture. *Sustain. Comput. Inform. Syst.* **2023**, *39*, 100898. [CrossRef]
6. Padmanaban, S.; Nasab, M.A.; Shiri, M.E.; Javadi, H.H.S.; Nasab, M.A.; Zand, M.; Samavat, T. The role of Internet of Things in smart homes. In *Artificial Intelligence-Based Smart Power Systems*; Wiley: Hoboken, NJ, USA, 2022; Chapter 13.
7. Evans, D. The internet of things: How the next evolution of the internet is changing everything. *Cisco Int. J. Internet* **2011**, *3*, 123–132.
8. Fahrurozi, M.; Tarigan, S.A.; Alam Tanjung, M.; Mutijarsa, K. The Use of ISO/IEC 27005: 2018 for Strengthening Information Security Management (A Case Study at Data and Information Center of Ministry of Defence). In Proceedings of the 2020 12th International Conference on Information Technology and Electrical Engineering (ICITEE), Yogyakarta, Indonesia, 6–8 October 2020.
9. Ahmed, F.; Ko, Y. Mitigation of black hole attacks in Routing Protocol for Low Power and Lossy Networks. *Secur. Commun. Netw.* **2016**, *9*, 5143–5154. [CrossRef]
10. Rawlinson, K. *HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack*; HP Advisory: Singapore, 2014.
11. Akram, H.; Konstantas, D.; Mahyoub, M. A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model. *Int. J. Adv. Comput. Sci. Appl.* **2018**, *9*, 355–373. [CrossRef]
12. Ahemd, M.M.; Shah, M.A.; Wahid, A. IoT security: A layered approach for attacks & defenses. In Proceedings of the 2017 International Conference on Communication Technologies (ComTech), Rawalpindi, Pakistan, 19–21 April 2017; pp. 104–110.
13. Ahlawat, B.; Sangwan, A.; Sindhu, V. IoT system model challenges and threats. *Int. J. Sci. Technol. Res.* **2020**, *9*, 6771–6776.
14. Ali, W.; Dustgeer, G.; Awais, M.; Shah, M.A. IoT based smart home: Security challenges, security requirements and solutions. In Proceedings of the 2017 23rd International Conference on Automation and Computing (ICAC), Huddersfield, UK, 7–8 September 2017; pp. 1–6.
15. Gupta, B.B.; G Arachchilage, N.A.; Psannis, K.E. Defending against phishing attacks: Taxonomy of methods, current issues and future directions. *Telecommun. Syst.* **2018**, *67*, 247–267. [CrossRef]
16. Hatzivasilis, G.; Ioannidis, S.; Smyrlis, M.; Spanoudakis, G.; Frati, F.; Goeke, L.; Hildebrandt, T.; Tsakirakis, G.; Oikonomou, F.; Leftheriotis, G.; et al. Modern Aspects of Cyber-Security Training and Continuous Adaptation of Programmes to Trainees. *Appl. Sci.* **2020**, *10*, 5702. [CrossRef]
17. Smyrlis, M.; Somarakis, I.; Spanoudakis, G.; Hatzivasilis, G.; Ioannidis, S. CYRA: A Model-Driven Cyber Range Assurance Platform. *Appl. Sci.* **2021**, *11*, 5165. [CrossRef]
18. Zhu, P.; Hu, J.; Li, X.; Zhu, Q. Using Blockchain Technology to Enhance the Traceability of Original Achievements. *IEEE Trans. Eng. Manag.* **2023**, *70*, 1693–1707. [CrossRef]
19. Touqeer, H.; Zaman, S.; Amin, R.; Hussain, M.; Al-Turjman, F.; Bilal, M. Smart home security: Challenges, issues and solutions at different IoT layers. *J. Supercomput.* **2021**, *77*, 14053–14089. [CrossRef]
20. Almusaylim, Z.A.; Zaman, N. A review on smart home present state and challenges: Linked to context-awareness internet of things (IoT). *Wirel. Netw.* **2019**, *25*, 3193–3204. [CrossRef]
21. Bugeja, J.; Jacobsson, A.; Davidsson, P. On privacy and security challenges in smart connected homes. In Proceedings of the 2016 European Intelligence and Security Informatics Conference (EISIC), Uppsala, Sweden, 17–19 August 2016; pp. 172–175.
22. Gavra, V.D.; Dobra, I.M.; Pop, O.A. A survey on threats and security solutions for IoT. In Proceedings of the 2020 43rd International Spring Seminar on Electronics Technology (ISSE), Demanovska Valley, Slovakia, 14–15 May 2020; pp. 1–5.
23. Geneiatakis, D.; Kounelis, I.; Neisse, R.; Nai-Fovino, I.; Steri, G.; Baldini, G. Security and privacy issues for an IoT based smart home. In Proceedings of the 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 22–26 May 2017; pp. 1292–1297.
24. Kamrul, I.; Shen, W.; Wang, X. Security and privacy considerations for wireless sensor networks in smart home environments. In Proceedings of the 2012 IEEE 16th International Conference on Computer Supported Cooperative Work in Design (CSCWD), Wuhan, China, 23–25 May 2012; pp. 626–633.

25. Uand, J.; Sun, L. A Comprehensive Survey of Security Issues of Smart Home System: "Spear" and "Shields," Theory and Practice. *IEEE Access* **2022**, *10*, 67–192.
26. Dahmen, J.; Cook, D.J.; Wang, X.; Honglei, W. Smart Secure Homes: A Survey of Smart Home Technologies that Sense, Assess, and Respond to Security Threats. *J. Reliab. Intell. Environ.* **2017**, *3*, 83–98. [CrossRef]
27. Bastos, D.; Shackleton, M.; El-Moussa, F. Internet of Things: A Survey of Technologies and Security Risks in Smart Home and City Environments. In Proceedings of the Living in the Internet of Things: Cybersecurity of the IoT, London, UK, 28–29 March 2018.
28. Gendreau, A.A.; Moorman, M. Survey of intrusion detection systems towards an end to end secure internet of things. In Proceedings of the 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), Vienna, Austria, 22–24 August 2016; pp. 84–90.
29. Faisal, E.M.; Awad, A.I.; Hamed, H.F.A. Intrusion detection systems for IoT-based smart environments: A survey. *J. Cloud Comput.* **2018**, *7*, 1–20.
30. Datta, P.; Sharma, B. A survey on IoT architectures, protocols, security and smart city based applications. In Proceedings of the 2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Delhi, India, 3–5 July 2017; pp. 1–5.
31. Sivaraman, V.; Gharakheili, H.H.; Vishwanath, A.; Boreli, R.; Mehani, O. Network-level security and privacy control for smart-home IoT devices. In Proceedings of the 2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Abu Dhabi, United Arab Emirates, 19–21 October 2015; pp. 1–5.
32. Isam, W.; Thomson, C.; Ghaleb, B. An RPL based optimal sensors placement in pipeline monitoring WSNs. In *International Conference on Emerging Technologies and Intelligent Systems*; Springer: Cham, Switzerland, 2021.
33. Li, H.; Chen, Y.; He, Z. The survey of RFID attacks and defenses. In Proceedings of the 2012 8th International Conference on Wireless Communications, Networking and Mobile Computing, Shanghai, China, 21–23 September 2012.
34. Yoon, S.; Park, H.; Yoo, H.S. Security issues on smarthome in IoT environment. In *Computer Science and Its Applications*; Springer: Berlin/Heidelberg, Germany, 2015; pp. 691–696.
35. Fariha, K.; Gawade, A. Secure Data Management in Smart Meter as an Application of IoT. *Int. J. Sci. Res. (IJSR)* **2016**, *5*, 1335–1337.
36. Kim, J.T.S. Analyses of Open Security Issues for Smart Home and Sensor Network Based on Internet of Things. *IoT Appl. Comput.* **2022**, *11*, 179–196.
37. Karlof, C.; Wagner, D. Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad Hoc Netw.* **2003**, *1*, 293–315. [CrossRef]
38. Gill, R.K.; Sachdeva, M. Detection of hello flood attack on LEACH in wireless sensor networks. In *Next-Generation Networks*; Springer: Singapore, 2018; pp. 377–387.
39. Arabo, A.; Pranggono, B. Mobile malware and smart device security: Trends, challenges and solutions. In Proceedings of the 2013 19th International Conference on Control Systems and Computer Science, Bucharest, Romania, 29–31 May 2013; pp. 1–6.
40. Zhu, P.; Zhang, H.; Shi, Y.; Xie, W.; Pang, M.; Shi, Y. A novel discrete conformable fractional grey system model for forecasting carbon dioxide emissions. In *Environment, Development and Sustainability*; Springer: Berlin/Heidelberg, Germany, 2024; pp. 1–29.
41. Xu, X.; Chen, J.; Zhang, L.; Zhang, Z. Investigating smart home assistant security: A systematic literature review. *IEEE Access* **2020**, *8*, 186500–186512.
42. Santani, A.; Gangaramani, M.; Chopra, B.; Choudhary, P.; Samdani, K. An overview of architecture and security issues of a smart TV. In Proceedings of the 6th International Conference on Communication and Electronics Systems (ICCES-2021), Coimbatre, India, 8–10 July 2021; pp. 1835–1843.
43. De Guzman, J.A.; Thilakarathna, K.; Seneviratne, A. Security and Privacy Approaches in Mixed Reality: A Literature Survey. *ACM Comput. Surv.* **2019**, *52*, 1–37. [CrossRef]
44. Abdi, N.; Ramokapane, K.M.; Such, J.M. More than smart speakers: Security and privacy perceptions of smart home personal assistants. In Proceedings of the 15th Symposium on Usable Privacy and Security (SOUPS 2019), USENIX Association, Santa Clara, CA, USA, 11–13 August 2019; pp. 451–466.
45. Zhang, L.; Wang, X.; Tan, Z.; Chen, J.; Xu, X.; Zhang, Z. Voice hacking: Evaluating voice-controlled smart home assistant's vulnerability against replay attacks. *IEEE Internet Things J.* **2021**, *8*, 7319–7330.
46. Zhang, Z.; Chen, J. Voice assistant security: A review of attack scenarios and defenses. *IEEE Secur. Priv.* **2019**, *17*, 22–29.
47. Xiao, Y.; Jiang, C.; Huang, D.; Liang, K. Secure and efficient access control for smart home assistant. *J. Ambient. Intell. Humaniz. Comput.* **2021**, *12*, 4545–4554.
48. Obaid, A. Assessment of Smart Home Assistants as an IoT. *Int. J. Comput. Inf. Manuf. (IJCIM)* **2021**, *1*, 18–36. [CrossRef]
49. Alam, I.; Khusro, S.; Naeem, M. A review of smart TV: Past, present, and future. In Proceedings of the International Conference on Open Source Systems and Technologies (ICOSST), Lahore, Pakistan, 5 February 2018; pp. 35–41.
50. Bachy, Y.; Basse, F.; Nicomette, V.; Alata, E.; Kaaniche, M.; Courrege, J.; Lukjanenko, P. Smart-TV security analysis: Practical experiments. In Proceedings of the 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, Rio de Janeiro, Brazil, 22–25 June 2015; pp. 497–504.
51. Bao, L.; Wu, S.; Yu, S.; Huang, J. Client-side Security Assessment and Security Protection Scheme for Smart TV Network. In Proceedings of the 6th International Conference on Computer and Communications, Chengdu, China, 11–14 December 2020; pp. 573–578.

52. Zhang, Y.; Ma, S.; Chen, T.; Li, J.; Deng, R.H.; Bertino, E. EvilScreen Attack: Smart TV Hijacking via Multi-channel Remote Control Mimicry. *IEEE Trans. Dependable Secur. Comput.* **2023**, *21*, 1544–1556. [CrossRef]
53. Claverie, T.; Lopes Esteves, J.; Kasmi, C. Smart TVs: Security of DVB-T. In Proceedings of the Information and Communications Technology Security Symposium (SSTIC), Rennes, France, 14 June 2018; pp. 73–106.
54. Aluri, D.C. Smart lock systems: An overview. *Int. J. Comput. Appl.* **2020**, *177*, 40–43.
55. Kalbo, N.; Mirsky, Y.; Shabtai, A.; Elovici, Y. The security of IP-Based video surveillance systems. *Sensors* **2020**, *20*, 4806. [CrossRef]
56. Nguyen, T. A deep look into privacy and security of vacuum robot. In Proceedings of the 20th Annual Cybersecurity & Awareness Fair (CyberFair), Pomona, CA, USA, 17 October 2024; pp. 1–7.
57. Ronen, E.; Shamir, A. Extended Functionality Attacks on IoT Devices: The Case of Smart Lights. In Proceedings of the IEEE European Symposium on Security and Privacy (EuroS&P), Saarbruecken, Germany, 21–24 March 2016; pp. 1–10. [CrossRef]
58. Huchuk, B.; Sanner, S.; O'Brien, W. Development and evaluation of data-driven controls for residential smart thermostats. *Energy Build.* **2021**, *249*, 111201. [CrossRef]
59. Hariadi, R.R.; Yuniarti, A.; Kuswardayan, I.; Herumurti, D.; Arifiani, S.; Yunanto, A.A. Termo: Smart air conditioner controller integrated with temperature and humidity sensor. In Proceedings of the 12th International Conference on Information & Communication Technology and System (ICTS), Surabaya, Indonesia, 18 July 2019; pp. 1–6. [CrossRef]
60. Reid, S.E.; Abdulrazak, B.; Alas, M. Proof of Concept Evaluation for an Intelligent Oven. *Enhanc. Qual. Life Smart Living* **2017**, *10461*, 161–172.
61. Nasir, H.; Aziz, W.B.W.; Ali, F.; Kadir, K.; Khan, S. The Implementation of IoT based Smart Refrigerator System. In Proceedings of the 2nd International Conference on Smart Sensors and Application (ICSSA), Kuching, Malaysia, 24–26 July 2018; pp. 48–52.
62. Gomes, L.; Sousa, F.; Vale, Z. An Intelligent Smart Plug with Shared Knowledge Capabilities. *Sensors* **2018**, *18*, 3961. [CrossRef] [PubMed]
63. Horák, T.; Huraj, L. Smart Thermostat as a Part of IoT Attack. In Proceedings of the 8th Computer Science On-line Conference, Cybernetics and Automation Control Theory Methods in Intelligent Algorithms (AISC), Zlin, Czech Republic, 24–27 April 2019; Volume 3, pp. 156–163.
64. Wang, A.; Nirjon, S. A False Sense of Home Security—Exposing the Vulnerability in Away Mode of Smart Plugs. In Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kyoto, Japan, 11–15 March 2019; pp. 316–321. [CrossRef]
65. Liu, P.; Ji, S.; Fu, L.; Lu, K.; Zhang, X.; Qin, J.; Wang, W.; Chen, W. How IoT re-using threatens your sensitive data: Exploring the User-Data disposal in used IoT devices. In Proceedings of the IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 21–25 May 2023; pp. 1–17. [CrossRef]
66. Shuhaiber, A.; Ahim Mashal, I. Understanding users' acceptance of smart homes. *Technol. Soc.* **2010**, *58*, 1011109. [CrossRef]
67. Këpuska, V.; Bohouta, G. Next-generation of virtual personal assistants (Microsoft Cortana, Apple Siri, Amazon Alexa and Google Home). In Proceedings of the IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 8–10 January 2018; pp. 1–8.
68. Fruchter, N.; Liccardi, I. Consumer Attitudes Towards Privacy and Security in Home Assistants. In Proceedings of the CHI Conference on Human Factors in Computing Systems, New York, NY, USA, 21–26 April 2018; Article LBW050. pp. 1–6. [CrossRef]
69. Lei, X.; Tu, G.; Liu, A.X.; Li, C.; Xie, T. The Insecurity of Home Digital Voice Assistants-Vulnerabilities, Attacks and Countermeasures. In Proceedings of the IEEE Conference on Communications and Network Security (CNS), Beijing, China, 30 May–1 June 2018; pp. 1–9. [CrossRef]
70. Sudharsan, B.; Corcoran, P.; Ali, M.I. Smart speaker design and implementation with biometric authentication and advanced voice interaction capability. In Proceedings of the AIAI Irish Conference on Artificial Intelligence and Cognitive Science, Galway, Ireland, 5–6 December 2019; pp. 1–14.
71. Corbett, C.F.; Combs, E.M.; Wright, P.J.; Owens, O.L.; Stringfellow, I.; Nguyen, T.; Van Son, C.R. Virtual Home Assistant Use and Perceptions of Usefulness by Older Adults and Support Person Dyads. *Int. J. Environ. Res. Public Health* **2021**, *18*, 1113. [CrossRef] [PubMed]
72. Diogo Vieira, A.; Leite, H.; Vitória Lachowski Volochtchu, A.K. The impact of voice assistant home devices on people with disabilities: A longitudinal study. *Technol. Forecast. Soc. Change* **2022**, *184*, 121961. [CrossRef]
73. Triyono, L.; Yudantoro, T.R.; Sukamto, S.; Hestinigsih, I. VeRO: Smart home assistant for blind with voice recognition. *Mater. Sci. Eng.* **2021**, *1108*, 012016. [CrossRef]
74. Beirl, D.; Rogers, Y.; Yuill, N. "Using Voice Assistant Skills in Family Life. In Proceedings of the International Conference on Computer Supported Collaborative Learning—A Wide Lens: Combining Embodied, Enactive, Extended, and Embedded Learning in Collaborative Settings (CSCL), Lyon, France, 17–21 June 2019; pp. 1–8.
75. Zhu, P.; Miao, C.; Wang, Z.; Li, X. Informational cascade, regulatory focus and purchase intention in online flash shopping. *Electron. Commer. Res. Appl.* **2023**, *62*, 16474–16496. [CrossRef]
76. Edu, J.S.; Such, J.M.; Suarez-Tangil, G. Smart home personal assistants: A security and privacy review. *ACM Comput. Surv.* **2019**, *53*, 116. [CrossRef]
77. Qamar, S.; Anwar, Z.; Afzal, M. A systematic threat analysis and defense strategies for the metaverse and extended reality systems. *Comput. Secur.* **2023**, *128*, 103127. [CrossRef]

78. Duezguen, R.; Mayer, P.; Das, S.; Volkamer, M. Towards Secure and Usable Authentication for Augmented and Virtual Reality Head-Mounted Displays. In Proceedings of the Who Are You?! Adventures in Authentication (WAY), Virtual Event, 7 August 2020; pp. 1–6.
79. Stephenson, S.; Pal, B.; Fan, S.; Fernandes, E.; Zhao, Y.; Chatterjee, R. SoK: Authentication in augmented and virtual reality. In Proceedings of the IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 22–26 May 2022; pp. 267–284. [CrossRef]
80. Ali, M.; Naeem, F.; Kaddoum, G.; Hossain, E. Metaverse communications, networking, security, and applications: Research issues, State-of-the-Art, and future directions. *IEEE Commun. Surv. Tutor.* **2024**, *26*, 1238–1278. [CrossRef]
81. Buldeo Rai, H.; Verlinde, S.; Macharis, C. Unlocking the failed delivery problem? Opportunities and challenges for smart locks from a consumer perspective. *Res. Transp. Econ.* **2021**, *87*, 100753. [CrossRef]
82. Ho, G.; Leung, D.; Mishra, P.; Hosseini, A.; Song, D.; Wagner, D. Smart Locks: Lessons for Securing Commodity Internet of Things Devices. In Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security (ASIA CCS), Xi'an, China, 30 May–3 June 2016; pp. 461–472.
83. De Camargo Silva, L.; Samaniego, M.; Deters, R. IoT and Blockchain for Smart Locks. In Proceedings of the 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 17–19 October 2019; pp. 262–269.
84. Nadiya, U.; Ilham Rizqyawan, M.; Mahnedra, O. Blockchain-based Secure Data Storage for Door Lock System. In Proceedings of the 4th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE), Yogyakarta, Indonesia, 20–21 November 2019; pp. 140–144.
85. Raizada, P.; Gupta, S.; Das, M.; Rastogi, P.; Arora, D. Smart Lock System using IoT, Embedded & Machine Learning. In Proceedings of the 7th International conference for Convergence in Technology (I2CT), Mumbai, India, 7–9 April 2022; pp. 1–8.
86. Hazazi, H.; Shehab, M. Exploring the Usability, Security, and Privacy of Smart Locks from the Perspective of the End User. In Proceedings of the 9th Symposium on Usable Privacy and Security, USENIX, Anaheim, CA, USA, 7–8 August 2023; pp. 559–577.
87. Pandya, S.; Ghayvat, H.; Kotecha, K.; Awais, M.; Akbarzadeh, S.; Gope, P.; Mukhopadhyay, S.C.; Chen, W. Smart home anti-theft system: A novel approach for near real-time monitoring and smart home security for wellness protocol. *Appl. Syst. Innov.* **2018**, *1*, 42. [CrossRef]
88. Abdalla, P.A.; Varol, C. Testing IoT security: The case study of an IP camera. In Proceedings of the 8th International Symposium on Digital Forensics and Security (ISDFS), Beirut, Lebanon, 1–2 June 2020; pp. 1–5.
89. Tekeoglu, A.; Saman Tosun, A. Investigating security and privacy of a cloud-based wireless IP camera: NetCAM. In Proceedings of the 24th International Conference on Computer Communication and Networks (ICCCN), Las Vegas, NV, USA, 3–6 August 2015; pp. 1–6.
90. Stolojescu-Crisan, C.; Crisan, C.; Butunoi, B. Access control and surveillance in a smart home. *High-Confid. Comput.* **2022**, *2*, 1–9. [CrossRef]
91. Wan, Y.; Xu, K.; Xue, G.; Wang, F. IoTArgos: A multi-layer security monitoring system for Internet-of-Things in smart homes. In Proceedings of the IEEE Conference on Computer Communications (INFOCOM), Toronto, ON, Canada, 6–9 July 2020; pp. 1–10.
92. Sami, S.; Dai, Y.; Tan, S.R.X.; Roy, N.; Han, J. Spying with your robot vacuum cleaner: Eavesdropping via lidar sensors. In Proceedings of the 18th ACM Conference on Embedded Networked Sensor Systems (SenSys'20), Virtual Event, Japan, 16–19 November 2020; pp. 1–14.
93. *ISO/IEC 30141:2018*; Internet of Things (IoT) Reference Architecture. 2018. Available online: https://www.iso.org/standard/65695.html (accessed on 19 February 2024).
94. Kim, S. *IEEE 2413-2029*; IEEE Standard for an Architectural Framework for the Internet of Things (IoT). IEEE Standards Association, 2019. Available online: https://standards.ieee.org/ieee/2413/6226/ (accessed on 19 February 2024).
95. Iiconsortium. The Industrial Internet Reference Architecture. Industry IoT Consortium. 2022. Available online: https://www.iiconsortium.org/iira/ (accessed on 19 February 2024).
96. OCF. OCF Specification 2.2.7. Open Connectivity Foundation, 2021. Available online: https://openconnectivity.org/developer/specifications/ (accessed on 19 February 2024).
97. NIST. NIST Cybersecurity Framework 2.0. 2024. Available online: https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-20/ipd (accessed on 19 February 2024).
98. Vo, J. NIST SP 800-13–Network of Things. NIST, 2016. Available online: https://csrc.nist.gov/pubs/sp/800/183/final (accessed on 19 February 2024).
99. Wu, M.; Lu, T.J.; Ling, F.Y.; Sun, J.; Du, H.Y. Research on the architecture of Internet of Things. In Proceedings of the 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), Chengdu, China, 20–22 August 2010; pp. 484–487.
100. Khattak, H.A.; Shah, M.A.; Khan, S.; Ali, I.; Imran, M. Perception layer security in Internet of Things. *Futur. Gener. Comput. Syst.* **2019**, *100*, 144–164. [CrossRef]
101. Li, S.; Tryfonas, T.; Li, H. The internet of things: A security point of view. *Internet Res.* **2016**, *26*, 337–359. [CrossRef]
102. Sethi, P.; Sarangi, S.R. Internet of things: Architectures, protocols, and applications. *J. Electr. Comput. Eng.* **2017**, *2017*, 1–25. [CrossRef]

103. Suo, H.; Wan, J.; Zou, C.; Liu, J. Security in the internet of things: A review. In Proceedings of the 2012 International Conference on Computer Science and Electronics Engineering, Hangzhou, China, 23–25 March 2012; Volume 3, p. 373. [CrossRef]
104. Ghafir, I.; Prenosil, V.; Alhejailan, A.; Hammoudeh, M. Social engineering attack strategies and defence approaches. In Proceedings of the 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), Vienna, Austria, 22–24 August 2016; pp. 145–149.
105. He, D.; Ye, R.; Chan, S.; Guizani, M.; Xu, Y. Privacy in the internet of things for smart healthcare. *IEEE Commun. Mag.* **2018**, *56*, 38–44. [CrossRef]
106. Kozlov, D.; Veijalainen, J.; Ali, Y. Security and privacy threats in IoT architectures. In Proceedings of the 7th International Conference on Body Area Networks (BODYNETS), Oslo, Norway, 24–26 September 2012; pp. 1–7.
107. Xu, X. Study on security problems and key technologies of the internet of things. In Proceedings of the 2013 International Conference on Computational and Information Sciences, Shiyang, China, 21–23 June 2013. [CrossRef]
108. Nirmal, K.; Janet, B.; Kumar, R. Analyzing and eliminating phishing threats in IoT, network and other web applications using iterative intersection. *Peer-to-Peer Netw. Appl.* **2021**, *14*, 2327–2339. [CrossRef]
109. Whittaker, C.; Ryner, B.; Nazif, M. Large-scale automatic classification of phishing pages. In Proceedings of the Network and Distributed System Security Symposium (Ndss), San Diego, CA, USA, 28 February–3 March 2010; pp. 1–14.
110. Deogirikar, J.; Vidhate, A. Security attacks in IoT: A survey. In Proceedings of the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 10–11 February 2017; pp. 32–37.
111. Wei, D.; Qiu, X. Status-based detection of malicious code in Internet of Things (IoT) devices. In Proceedings of the 2018 IEEE Conference on Communications and Network Security (CNS), Beijing, China, 30 May–1 June 2018; pp. 1–7.
112. Sharma, P.; Zawar, S.; Pati, S.B. Ransomware analysis: Internet of Things (Iot) security issues challenges and open problems in the context of worldwide scenario of security of systems and malware attacks. *Manag. J. Innov. Res. Sci. Eng. (IJIRSE)* **2016**, *2*, 177–184.
113. Stamelos, I.; Hatzivasilis, G.; Ioannidis, S. Active HoneyFiles for Ransomware Encryption Mitigation. In Proceedings of the IEEE International Conference on Cyber Security and Resilience (IEEE CSR) Workshops, London, UK, 2–4 September 2024; pp. 1–8.
114. Cesare, S. Breaking the security of physical devices. In Proceedings of the Black Hat USA 2014, Las Vegas, NV, USA, 2–7 August 2014; pp. 1–7.
115. Hossain, M.M.; Fotouhi, M.; Hasan, R. Towards an analysis of security issues, challenges, and open problems in the internet of things. In Proceedings of the 2015 IEEE World Congress on Services, New York, NY, USA, 27 June–2 July 2015; pp. 21–28.
116. Varga, P.; Plosz, S.; Soos, G.; Hegedus, C. Security threats and issues in automation IoT. In Proceedings of the 2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS), Trondheim, Norway, 31 May–2 June 2017; pp. 1–6.
117. Hassija, V.; Chamola, V.; Saxena, V.; Jain, D.; Goyal, P.; Sikdar, B. A survey on IoT security: Application areas, security threats, and solution architectures. *IEEE Access* **2019**, *7*, 82721–82743. [CrossRef]
118. Zhao, W.; Yang, S.; Luo, X. On threat analysis of IoT-based systems: A survey. In Proceedings of the 2020 IEEE International Conference on Smart Internet of Things (SmartIoT), Beijing, China, 14–16 August 2020; pp. 205–212.
119. Kim, D. Cyber security issues imposed on nuclear power plants. *Ann. Nucl. Energy.* **2014**, *65*, 141–143. [CrossRef]
120. Denning, D.E. Stuxnet: What has changed? *Future Internet* **2012**, *4*, 672–687. [CrossRef]
121. Ko, E.; Kim, T.; Kim, H. Management platform of threats information in IoT environment. *J. Ambient. Intell. Humaniz. Comput.* **2018**, *9*, 1167–1176. [CrossRef]
122. Ganguly, P.; Nasipuri, M.; Dutta, S. A novel approach for detecting and mitigating the energy theft issues in the smart metering infrastructure. *Technol. Econ. Smart Grids Sustain. Energy.* **2018**, *3*, 1–11. [CrossRef]
123. Alnaeli, S.M.; Sarnowski, M.; Aman, M.S.; Abdelgawad, A.; Yelamarthi, K. Vulnerable C/C++ code usage in IoT software systems. In Proceedings of the 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, USA, 12–14 December 2016; pp. 348–352.
124. Werner, M.; Unterluggauer, T.; Schaffenrath, D.; Mangard, S. Sponge-based control-flow protection for IoT devices. In Proceedings of the 2018 IEEE European Symposium on Security and Privacy (EuroS&P), London, UK, 24–26 April 2018; pp. 214–226.
125. Mujica, G.; Portilla, J. Distributed reprogramming on the edge: A new collaborative code dissemination strategy for IoT. *Electronics* **2019**, *8*, 267. [CrossRef]
126. Abbas, S.G.; Vaccari, I.; Hussain, F.; Zahid, S.; Fayyaz, U.U.; Shah, G.A.; Bakhshi, T.; Cambiaso, E. Identifying and Mitigating Phishing Attack Threats in IoT Use Cases Using a Threat Modelling Approach. *Sensors* **2021**, *21*, 4816. [CrossRef] [PubMed]
127. Li, X.; Zhang, D.; Wu, B. Detection method of phishing email based on persuasion principle. In Proceedings of the IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chongqing, China, 12–14 June 2020; pp. 571–574. [CrossRef]
128. Nishikawa, H.; Yamamoto, T.; Harsham, B.; Wang, Y.; Uehara, K.; Hori, C.; Iwasaki, A.; Kawauchi, K.; Nishigaki, M. Analysis of Malicious Email Detection using Cialdini's Principles. In Proceedings of the 15th Asia Joint Conference on Information Security (AsiaJCIS), Taipei, Taiwan, 20–21 August 2020; pp. 137–142.
129. Sonowal, G. Phishing Email Detection Based on Binary Search Feature Selection. *SN Comput. Sci.* **2020**, *1*, 191. [CrossRef] [PubMed]
130. Sahingoz, O.K.; Buber, E.; Demir, O.; Diri, B. Machine learning based phishing detection from URLs. *Expert. Syst. Appl.* **2019**, *117*, 345–357. [CrossRef]

131. Ficco, M. Detecting IoT malware by Markov chain behavioral models. In Proceedings of the IEEE International Conference on Cloud En-gineering (IC2E), Prague, Czech Republic, 24–27 June 2019; pp. 229–234. [CrossRef]
132. Sharmeen, S.; Huda, S.; Abawajy, J.H.; Ismail, W.N.; Hassan, M.M. Malware threats and detection for industrial Mobile-IoT networks. *IEEE Access* **2018**, *6*, 15941–15957. [CrossRef]
133. Wang, W.; Zhao, M.; Gao, Z.; Xu, G.; Xian, H.; Li, Y.; Zhang, X. Constructing features for detecting android malicious applications: Issues, taxonomy and directions. *IEEE Access* **2019**, *7*, 67602–67631. [CrossRef]
134. Nimmy, K.; Sankaran, S.; Achuthan, K. A novel multi-factor authentication protocol for smart home environments. In *Information Systems Security (ICISS)*; Springer: Cham, Germany, 2018; Volume 11281, pp. 44–63.
135. Nimmy, K.; Sankaran, S.; Achuthan, K.; Calyam, P. Lightweight and privacy-preserving remote user authentication for smart homes. *IEEE Access* **2022**, *10*, 176–190. [CrossRef]
136. Nagy, R.; Németh, K.; Papp, D.; Buttyán, L. Rootkit detection on embedded IoT devices. *Acta Cybern.* **2021**, *25*, 369–400. [CrossRef]
137. Haney, J.M.; Furman, S.M. Smart Home Updates: User Perceptions and Experiences. In Proceedings of the Symposium on Security and Privacy (SP), San Francisco, CA, USA, 21–25 May 2023; pp. 1–5.
138. Haney, J.M.; Furman, S.M. Work in progress: Towards usable updates for smart home devices. In Proceedings of the Socio-Technical Aspects in Security and Trust (STAST), Virtual Event, 14 September 2020; Springer: Cham, Switzerland, 2021; Volume 12812, pp. 107–117.
139. Classen, J.; Chen, J.; Steinmetzer, D.; Hollick, M.; Knightly, E. The spy next door: Eavesdropping on high throughput visible light communications. In Proceedings of the 2nd International Workshop on Visible Light Communications Systems, New York, NY, USA, 11 September 2015; pp. 9–14.
140. Kaur, M.; Kalra, S. Security in IoT-Based smart grid through quantum key distribution. *Adv. Intell. Syst. Comput.* **2018**, *2*, 523–530. [CrossRef]
141. Fakhri, D.; Kusprasapta, M. Secure IoT communication using blockchain technology. In Proceedings of the 2018 international Symposzium on Electronics and Smart Devices (ISESD), Bandung, Indonesia, 23–24 October 2018; pp. 1–6.
142. Das, D.; Maity, S.; Nasir, S.B.; Ghosh, S.; Raychowdhury, A.; Sen, S. High efficiency power side-channel attack immunity using noise injection in attenuated signature domain. In Proceedings of the 2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), Mclean, VA, USA, 1–5 May 2017; pp. 62–67.
143. Siddiqui, S.T.; Alam, S.; Ahmad, R.; Shuaib, M. Security threats, attacks, and possible countermeasures in internet of things. *Lect. Notes Netw. Syst.* **2020**, 35–46. [CrossRef]
144. Hariri, R.H.; Fredericks, E.M.; Bowers, K.M. Uncertainty in big data analytics: Survey, opportunities, and challenges. *J. Big Data* **2019**, *6*, 1–16. [CrossRef]
145. Kanuparthi, A.; Karri, R.; Addepalli, S. Hardware and embedded security in the context of internet of things. In Proceedings of the 2013 ACM Workshop on Security, Privacy & Dependability for Cyber Vehicles, Berlin, Germany, 4 November 2013; pp. 61–64. [CrossRef]
146. Abrishamchi, M.N.; Abdullah, A.H.; Cheok, A.D.; Nikolic, P.K. A probability based hybrid energy-efficient privacy preserving scheme to encounter with wireless traffic snooping in smart home. In Proceedings of the 2nd EAI International Summit, Smart City 360°, Bratislava, Slovakia, 22–24 November 2017; pp. 1–10.
147. Zeng, X.; Martinez, T. A noise filtering method using neural networks. In Proceedings of the IEEE International Workshop on Soft Computing Techniques in Instrumentation, Measurement and Related Applications, Provo, UT, USA, 17 May 2003; pp. 26–31.
148. Li, Z.; Yin, X.; Geng, Z.; Zhang, H.; Li, P.; Sun, Y.; Zhang, H.; Li, L. Research on PKI-like Protocol for the Internet of Things. In Proceedings of the 2013 Fifth International Conference on Measuring Technology and Mechatronics Automation, Hong Kong, China, 16–17 January 2013; pp. 915–918.
149. Liu, Y.; Briones, J.; Zhou, R.; Magotra, N. Study of secure boot with a FPGA-based IoT device. In Proceedings of the 2017 IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS), Boston, MA, USA, 6–9 August 2017; pp. 1053–1056.
150. Arış, A.; Oktuğ, S.F.; Yalçın, S.B.Ö. Internet-of-Things security: Denial of service attacks. In Proceedings of the 2015 23rd Signal Processing and Communications Applications Conference (SIU), Malatya, Turkey, 16–19 May 2015; pp. 1–4.
151. Abhishek, N.V.; Tandon, A.; Lim, T.J.; Sikdar, B. Detecting forwarding misbehavior in clustered IoT networks. In Proceedings of the 14th ACM International Symposium on QoS and Security for Wireless and Mobile Networks, Montrea, QC, Canada, 28 October–2 November 2018; pp. 1–6. [CrossRef]
152. Ande, R.; Adebisi, B.; Hammoudeh, M.; Saleem, J. Internet of things: Evolution and technologies from a security perspective. *Sustain. Cities Soc.* **2020**, *54*, 101728. [CrossRef]
153. Ashibani, Y.; Mahmoud, Q.H. A behavior profiling model for user authentication in IoT networks based on app usage patterns. In Proceedings of the IECON 2018—44th Annual Conference of the IEEE Industrial Electronics Society, Washington, DC, USA, 21–23 October 2018; pp. 2841–2846. [CrossRef]
154. Hossain, M.; Riazul Islam, S.M.; Ali, F.; Kwak, K.; Hasan, R. An internet of things-based health prescription assistant and its security system design. *Futur. Gener. Comput. Syst.* **2018**, *82*, 422–439. [CrossRef]
155. Hussain, F.; Hussain, R.; Hassan, S.A.; Hossain, E. Machine learning in IoT security: Current solutions and future challenges. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1686–1721. [CrossRef]

156. Arora, A.; Kaur, A.; Bhushan, B.; Saini, H. Security concerns and future trends of internet of things. In Proceedings of the 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), Kannur, India, 5–6 July 2019; pp. 891–896.
157. Asif, W.; Ray, I.G.; Rajarajan, M. An attack tree based risk evaluation approach for the internet of things. In Proceedings of the 8th International Conference on the Internet of Things, Santa Barbara, CA, USA, 15–18 October 2018; pp. 1–8. [CrossRef]
158. Dwivedi, A.D.; Srivastava, G.; Dhar, S.; Singh, R. A decentralized Privacy-Preserving healthcare blockchain for IoT. *Sensors* **2019**, *19*, 326. [CrossRef]
159. Aziz, T.; Haq, E. Security challenges facing IoT layers and its protective measures. *Int. J. Comput. Appl.* **2018**, *179*, 31–35. [CrossRef]
160. Kim, Y.; Yoo, S.; Yoo, C. DAoT: Dynamic and energy-aware authentication for smart home appliances in Internet of Things. In Proceedings of the 2015 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 9–12 January 2015; pp. 196–197.
161. Kamel, S.O.; Hegazi, N.H. A proposed model of IoT security management system based on a study of internet of things (IoT) security. *Int. J. Sci. Eng. Res.* **2018**, *9*, 1227–1244.
162. Hatzivasilis, G.; Soultatos, O.; Chatziadam, P.; Fysarakis, K.; Askoxylakis, I.; Ioannidis, S.; Alexandris, G.; Katos, V.; Spanoudakis, G. WARDOG: Awareness detection watchdog for botnet infection on the host device. *IEEE Trans. Sustain. Comput.* **2019**, *4*, 1–15. [CrossRef]
163. Aliyu, F.; Sheltami, T.; Shakshuki, E.M. A detection and prevention technique for man in the middle attack in fog computing. *Procedia Comput. Sci.* **2018**, *141*, 24–31. [CrossRef]
164. Ameer, S.; Benson, J.; Sandhu, R. An Attribute-Based Approach toward a Secured Smart-Home IoT Access Control and a Comparison with a Role-Based Approach. *Information* **2022**, *13*, 60. [CrossRef]
165. Hatzivasilis, G.; Papaefstathiou, I.; Manifavas, C. SCOTRES: Secure Routing for IoT and CPS. *IEEE Internet Things J. (IoT)* **2017**, *4*, 2129–2141. [CrossRef]
166. Rajora, C.S.; Sharma, A. IoT Based Smart Home with Cutting-Edge Technology for IDS/IPS. In Proceedings of the 2nd International Conference on Advanced Technologies in Intelligent Control, Environment, Computing & Communication Engineering (ICATIECE), Bangalore, India, 16–17 December 2022; pp. 1–5.
167. Atlam, H.F.; Wills, G.B. IoT security, privacy, safety and ethics. In *Digital Twin Technologies and Smart Cities*; Springer: Cham, Switzerland, 2020; pp. 123–149.
168. Ida, I.B.; Jemai, A.; Loukil, A. A survey on security of IoT in the context of eHealth and clouds. In Proceedings of the 2016 11th International Design & Test Symposium (IDT), Hammamet, Tunisia, 18–20 December 2016; pp. 25–30.
169. Andrea, I.; Chrysostomou, C.; Hadjichristofi, G. Internet of Things: Security vulnerabilities and challenges. In Proceedings of the 2015 IEEE Symposium on Computers and Communication (ISCC), Larnaca, Cyprus, 6–9 July 2015; pp. 180–187.
170. Meng, S.; Gao, Z.; Li, Q.; Wang, H.; Dai, H.N.; Qi, L. Security-Driven hybrid collaborative recommendation method for cloud-based iot services. *Comput. Secur.* **2020**, *97*, 101950. [CrossRef]
171. Jayakumar, H.; Raha, A.; Kim, Y.; Sutar, S.; Lee, W.S.; Raghunathan, V. Energy-efficient system design for IoT devices. In Proceedings of the 2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC), Macao, China, 25–28 January 2016; pp. 298–301.
172. Kalra, N.; Sharma, A.; Kumar, N.; Singh, R.; Gehlot, A. Design and development of IoT-based transmission line monitoring system. In *Intelligent Communication, Control and Devices*; Springer: Singapore, 2018; pp. 465–471.
173. Dou, Z.; Si, G.; Lin, Y.; Wang, M. An adaptive resource allocation model with anti-jamming in IoT network. *IEEE Access* **2019**, *7*, 93250–93258. [CrossRef]
174. Choi, J.; Jin, S.I. Security threats in connected car environment and proposal of in-vehicle infotainment-based access control mechanism. In *Advanced Multimedia and Ubiquitous Engineering*; Springer: Singapore, 2018; pp. 383–388.
175. Rodrigues, L.; Guerreiro, J.; Correia, N. RELOAD/CoAP architecture for the federation of wireless sensor networks. *Peer-to-Peer Netw. Appl.* **2020**, *13*, 27–37. [CrossRef]
176. Jeyaselvi, M.; Sathya, M.; Suchitra, S.; Jafar Ali Ibrahim, S.; Kalyan Chakravarthy, N.S. SVM-Based Cloning and Jamming Attack Detection in IoT Sensor Networks. In *Advances in Information Communication Technology and Computing*; Springer: Singapore, 2022; Volume 392, pp. 461–471.
177. Mbarek, B.; Ge, M.; Pitner, T. Trust-Based Authentication for Smart Home Systems. In *Wireless Personal Communications*; Springer: Berlin/Heidelberg, Germany, 2021; Volume 117, pp. 2157–2172.