Computers & Security 117 (2022) 102677

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Survey on smart homes: Vulnerabilities, risks, and countermeasures

Badis Hammi[a,*], Sherali Zeadally[b], Rida Khatoun[c], Jamel Nebhen[d]

[a] EPITA Engineering School, France
[b] University of Kentucky, USA
[c] Institut Mines Telecom Paris, France
[d] Prince Sattam bin Abdulaziz University, KSA

ARTICLE INFO

Article history:
Received 24 September 2021
Revised 10 January 2022
Accepted 28 February 2022
Available online 4 March 2022

Keywords:
Home
IoT
Security
Vulnerability
Attack
Threat
Solution

ABSTRACT

Over the last few years, the explosive growth of Internet of Things (IoT) has revolutionized the way we live and interact with each other as well as with various types of systems and devices which form part of the Information Communication Technology (ICT) infrastructure. IoT is having a significant impact on various application domains including healthcare, smart home, transportation, energy, agriculture, manufacturing, and many others. We focus on the smart home environment which has attracted a lot of attention from both academia and industry recently. The smart home provides a lot of convenience to home users but it also opens up various risks that threaten both the security and privacy of the users. In contrast to previous works on smart home security and privacy, we present an overview of smart homes from both academic and industry perspectives. Next we discuss the security requirements, challenges and threats associated with smart homes. Finally, we discuss countermeasures that can be deployed to mitigate the identified threats.

1. Introduction

Internet of Things (IoT) has revolutionized humans' lives. Actually, IoT is pervasive in almost all fields of our daily lives (Gafurov and Chung, 2019; Hammi et al., 2017a; Park et al., 2019b). In this context, the Smart Home (SH) is an important area among the IoT use cases and its market and smart home technologies are continuously growing (Park et al., 2019a), especially after the strong interest of giant electronics hardware manufacturers such as *Samsung* and *LG* as well as famous IT companies such as *Google* and *Apple* (Withanage et al., 2014; Xu et al., 2016a). Consequently, numerous companies in the world focused their research and development on the smart home area. For example, one of the french telecommunications market leaders *Free*, has announced[1] its new product, which, in addition to Internet linking can also cooperate with numerous home's devices such as *Amazon Alexa* products, *Nest* products, numerous smart apps, smart TVs, the management of a smart surveillance system and many others.[2]

A smart home system is a set of devices which aim to provide security and comfort to its householders. However, the smart home's design can open up the door to numerous risks that range from exposing the privacy of householders to facilitating traditional crimes such as burglary by using video and audio feeds to identify houses with expensive items and then unlocking doors or disabling home security, or even worse tampering with healthcare appliances to physically harm people. In this context, in the 2018 *Web Summit*, researchers from *Avast lab* demonstrated how a hacker can access and control any connected smart home device.[3]

In summary, the demand for IoT devices, especially in the multi-billion-dollar residential consumer market has created a modern-day gold rush. Both new and established companies are trying to rush into the smart home market. However, it is more about production and cost than pragmatic security practices. Thus, smart homes security threats are exponentially increasing and will increase more in the future as more Internet-connected devices will be installed in the home. The security of smart homes is very important and more research is needed to protect the privacy and security of smart home occupants.

1.1. Research contributions of this work

Table 1 summarizes recently published surveys that have discussed various aspects of smart home security. We note that almost half of the existing works dates back to 2016 or before. Thus,

* Corresponding author.
E-mail addresses: badis.hammi@epita.fr (B. Hammi), szeadally@uky.edu (S. Zeadally), rida.khatoun@telecom-paris.fr (R. Khatoun), j.nebhen@psau.edu.sa (J. Nebhen).

[1] https://www.youtube.com/watch?v=FKquxJ-610s.
[2] https://www.youtube.com/watch?v=bVPRe03AMco.
[3] https://www.youtube.com/watch?v=iKBR18gxOKI.

https://doi.org/10.1016/j.cose.2022.102677
0167-4048/

Table 1
Comparison of existing surveys on smart home security.

Survey	Year	Focus on smart homes only ?	Considers smart homes from an industry perspective ?	Discusses security of smart homes ?	Analyses security solutions designed for smart homes ?	Limitations
Lee et al. (2014)	2014	Yes	No	Briefly	No	6 pages long, does not cover all the existing threats
Bugeja et al. (2016)	2016	Yes	No	Briefly	No	A 4 pages long survey does not cover security solutions, threats in depth
Lin and Bergmann (2016)	2016	No	No	Partially	Partially	Does not cover all the recent works published in the past 4 years
Chitnis et al. (2016)	2016	Yes	Yes	Briefly	No	7 pages long, has focused only on operating system security
Bastos et al. (2018)	2018	No	No	Briefly	No	Does not focus on smart homes and does not discuss security of smart homes
Mocrii et al. (2018)	2018	Yes	No	Briefly	No	The security of smart homes is discussed only briefly (in only two paragraphs)
Ali and Awad (2018)	2018	Yes	No	Partially	Partially	Does not cover the most recent security solutions and threats for smart homes reported in the last two years
Alrawi et al. (2019)	2019	Yes	Yes	Yes	Partially	Does not cover recent threats and solutions reported in the last two years
Shouran et al. (2019)	2019	Yes	No	Briefly	Briefly	6 pages long, does not cover all recent threats identified for smart homes
Edu et al. (2020)	2019	Yes	Yes	Yes	No	Studied Smart Personal Assistant only
Panwar et al. (2019)	2019	Yes	Yes	Yes	Partially	Only focuses on the security of communication protocols
Ahmed and Zeebaree (2021)	2021	Yes	No	Yes	Partially	Only classifies the works and does not discuss security problems/solutions from a technical perspective
Mohammad et al. (2021)	2021	Yes	No	Yes	Partially	Focuses on access control only
Rastogi et al. (2021)	2021	No	Yes	Briefly	No	Focuses on physical layer and hardware design of devices only
Our survey	2021	Yes	Yes	Yes	Yes	/

these works do not include many recent and current threats, issues and security solutions. As for the remaining surveys, they do not discuss the latest developments in smart home security in the last two years during which most of the works on smart homes have been published. Moreover, most recent publications on the topic of smart home security are fairly brief (typically 6 pages long) with many of them covering only a few security and threat aspects and cannot be considered to be extensive surveys. Finally, it is well-known that many of the commercial products of the smart home market are the origin of most well-known security flaws. Therefore, it is necessary to consider smart home system from an industry perspective which we do in this survey but has not been addressed by most related surveys published to date on the topic of smart home security.

For this work, we have used various sources of information to identify IoT vulnerabilities, threats, and other relevant security issues pertaining to smart homes. The sources used included many scholarly articles/papers, surveys, books, and case studies all of which were published within the past six years. Moreover, in this paper, we have focused solely on the smart home use case in order to provide an in-depth and comprehensive survey that covers, to the best of our knowledge, almost all the works on smart home security issues as well as the latest proposed solutions. We summarize the main contributions of this work as follows:

- We present an overview of smart home architectures (from both industry and academic perspectives) and we analyze related security threats.
- We propose a network/threat model for future research in the smart home security area.
- We discuss the security requirements and challenges associated with smart homes.
- We analyze the different security approaches applied to the smart home environment.
- Finally, we outline some countermeasures to mitigate the threats we have identified.

2. Overview on smart home systems

The smart home concept has evolved with the advances in other fields such as electronics, new information communication technologies, mobile applications, autonomous systems, virtualization, cloud computing, and so on. We define a smart home as a house equipped with a set of devices which are equipped with computation capabilities and communication technologies and interact with each other in order to achieve security, comfort, and convenience for home residents. These devices can also be controlled remotely by their users.

The current state of smart homes is a little far from the perfect scenario as described by *diynetwork.com*[4] *"Morning brings a graduated alarm that plays some of your favorite music. The volume builds slowly and the bedroom curtains gently part until you react and tell the alarm. Meanwhile, the bathroom floors are already warming in anticipation of your arrival, and the coffee-maker starts brewing up"*. Indeed, the current smart home systems represent a set of subsystems that are generally not fully autonomous and they focus on a specific task (e.g., smart vacuum, smart fridge, smart plant pot, intelligent virtual assistants, etc.) and do not really ensure strong cooperation with each other or support even limited cooperation due to the absence of a central autonomous control and command (C&C) system. Fig. 1 describes the end user view of a smart home.

[4] Home Automation Trends: http://www.diynetwork.com.

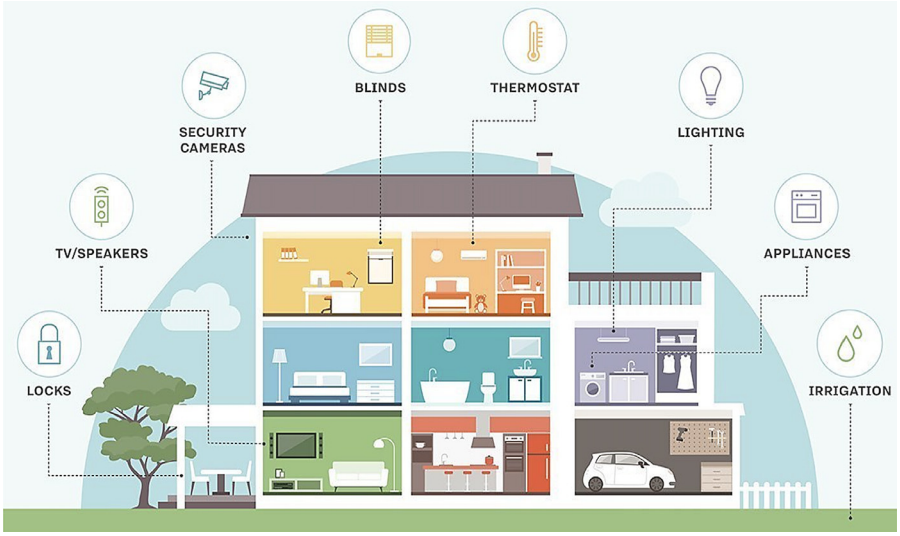

Fig. 1. End user view of a smart home Shea (July 2020).

2.1. Smart home services

There is a wide range of smart home services. We describe some use case scenarios.

Intelligent Virtual (Personal) Assistants (IVA): IVAs are hands-free, voice controlled devices that can achieve numerous tasks such as voice interaction, playing music, managing to-do lists, web browsing, setting alarms, placing orders and even controlling other devices such as smart locks, light bulbs, thermostats, etc. *Amazon Alexa, Google assistant, Apple Siri* and *Microsoft Cortana* are the most common and extensively used IVA systems (López et al., 2017).

For *Alexa*, the commands entry interface is a smart speaker called *Echo. Alexa* is receiving a lot of attention from devices manufacturers and software developers, especially after the announcement of its convergence with various devices, such as connected cars, smart fridges, and many robots in the *Consumer Electronics Show (CES) 2017* (Chung et al., 2017). Competitors such as *Google, Apple* and *Microsoft Cortana* also developed their smart speaker called *Google Assistant, HomePod* and *Invoke* respectively as a communication interface, which use natural language in addition to smart phones, pads or computers. Finally, in the same context, the Chinese giant *Xiaomi* also developed its own product as well as the Russian *Yandex* which is called *Alice*.[5]

Smart energy management: Smart grid is a concept that integrates information communication technologies and grid energy systems in order to achieve intelligent and efficient energy supply and consumption (Komninos et al., 2014; She et al., 2019; Stojkoska and Trivodaliev, 2017). In this context, the smart home system plays a key role in the interaction between the grid provider and the consumer (Viani et al., 2013). Devices such as smart meters can be deployed to monitor residents' activities. Then, recommendations can be provided in order to lower the energy cost (e.g., making some greedy home tasks in the time slots where the energy costs the less, lowering the power of some of the household appliances such as the fridge, the washing machine, and so on). In such a system, the information about energy consumption is automatically sent to the vendor.

Other than the smart grid, the estimation of space (room) occupation is a useful way for saving energy. Indeed, several works have investigated the possibility to make collaborate motion sensors and smart cameras with each other and electric devices such as light bulbs or heating systems in order to detect if persons are present in some location or not and then taking actions such as keeping or not keeping the light or heating on Viani et al. (2013), Byun et al. (2012).

Smart health and elderly management: A smart home represents a suitable environment for supporting healthcare services. It can be equipped with various sensors to enhance the detection of anomalies or behavioral changes (Viani et al., 2013). This opportunity has numerous benefits such as (1) lowering costs in comparison to institutional living or (2) keeping the patient with his/her family in a better social environment instead of being alone. Moreover, this smart home setup brings numerous benefits for elderly persons living alone. Smart speakers and screens can notify the elderly person when to take his/her medicine or any other task, alert the hospital or the paramedics if the resident fell and needs immediate attention. An autonomous system can help the resident if he/she forgets to close doors, curtains, to turn off the light, the oven, the water, and so on. It also allows adult children who might live elsewhere to participate in the care of their aging parent or to help him or her by remotely controlling the smart home devices.

Independent smart household appliances: There are many smart household devices which can be autonomous, programmable (schedulable) or can be remotely controlled through software applications. These devices provide household services such as comfort, security, housework, and others. For instance, smart surveillance cameras integrate image processing and classification to differentiate between people and animals before issuing an alarm. In the same context, smart alarms cooperate with motion sensors and smart surveillance cameras. There is another scenario called holiday mode that enables cooperation between smart alarms, sensors and cameras to track any suspicious motion, making the locks in *closed mode* as well as making the lights turn on and off to simulate a similar activity that occurs when the house residents are there. A smart home can also be equipped with a smart vacuum which can be scheduled or triggered remotely, a smart fridge, programmed to keep certain type of food in stock all the time. If this food is consumed, it sends a message to add it to the shopping list or orders it. A smart washing machine monitors the level of washing powder. If the level reaches a certain threshold, the washing machine sends a message to add it to the shopping list or orders it. A smart watering system for plants, can be scheduled or triggered remotely, and many other examples.

[5] https://market.yandex.ru/product--multimedia-platforma-yandex-stantsiia/1971204201.

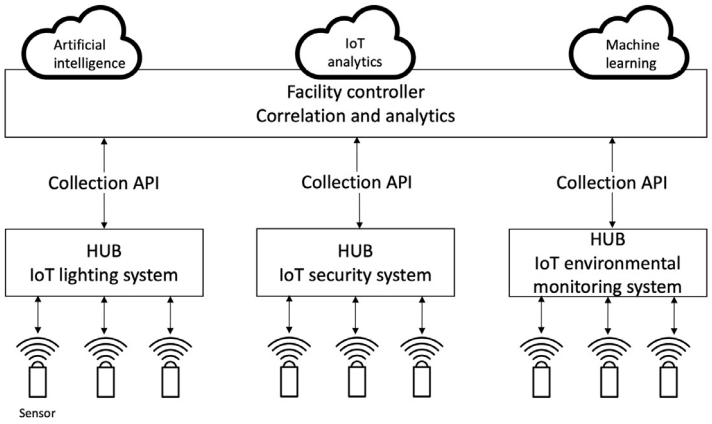

Fig. 2. Cloud based smart home architecture (Shea, July 2020).

2.2. Smart home architectures

2.2.1. Academic perspective

From an academic standpoint, there are two visions of smart home architectures:

1 - Centralized architecture: it requires the existence of a centralized decision unit, that receives and correlates data from the different sensors and devices. Then, according to the received information and/or the context, it takes decisions and triggers actions through messages and instructions to the appropriate devices. This centralized controller can either be (1) a hardware specific device which have adequate processing power, or (2) an application on the cloud. In both cases, the centralized device responsible for the collection of raw/processed data then processing/sending it to the cloud is called the Hub (She et al., 2019; Stojkoska and Trivodaliev, 2017).

Xu et al. (2016a) proposes a new architecture called Software Defined Smart Home, which applies the core idea of Software Defined Networks (SDN) (centralization, openness and virtualization) to the challenges (data aggregation, data processing, decision making, etc.) that smart homes face by dividing the ecosystem to three layers: (1) the **smart hardware layer** which includes the smart devices and sensors; (2) the **controller layer** which represents a centralized management entity. The controller layer is designed to shield the hardware details from the smart hardware layer, receiving and analyzing user demands, and managing the smart home automatically and intelligently. Moreover, the controller layer encapsulates all kinds of summary information and works with the external service layer; (3) The **external service layer** integrates the existing home service resources, offering smart home users with highly efficient, high-quality, and personalized services (Xu et al., 2016a).

2 - Autonomous architecture: this solution considers that each device is fully autonomous in sensing, collecting information, taking decisions, communicating with other devices and acting. In order to have a larger view and understanding of the environment, a device can cooperate with other devices. Autonomous devices can ensure the information processing locally if they have adequate resources locally or on the cloud if they do not. This solution does not exclude the possibility of remotely controlling some devices by users if they wish to do so. Fig. 2 describes a cloud based smart home architecture.

2.2.2. Industry perspective of the smart home

From an industry standpoint, the majority of smart home devices are independent devices that focus on a specific task in some pre-scheduled way (e.g., smart thermostat for heating, smart vacuum, and so on) or after being triggered remotely. However, leading information technology companies are developing newer systems that aim to integrate smart home devices in a centralized C&C environment. These systems are: easier to set up, cloud based and they are able to provide a programming framework for third-party developers to build applications that interact with the smart home devices in order to provide smart home benefits (Fernandes et al., 2016). As examples we cite *Samsung's SmartThings*[6], *Apples HomeKit*[7], *Vera Controls Vera3*[8], *Google Nest Weave*[9], *AllSeen Alliances*[10] *AllJoyn*[11], *Alibaba Smart Living*[12], *QQ IoT*[13] and *Xiaomi Mijia Aqara homekit*[14]. Some of these products use an IVA (in addition to a software application running on a smart phone or a computer) as a communication interface such as *Samsung's SmartThings* which can be controlled via *Alexa or Google home*, or the *Xiaomi Mijia Aqara* devices that can be controlled through the *Xiaomi* smart speaker. However, these systems are not fully autonomous. Indeed, the centralized control system, whether it is an IVA or a software application, only serves as an interface between the user (human) and the device. But, in the majority of cases, there are no autonomous reasoning and decision that take place. Fig. 3 depicts the generic architecture of current industrial smart home ecosystems. As described, we can note different independent and non cooperative home appliances (e.g., smart TV, smart thermostat, and so on) that mainly work in a prescheduled way and can be controlled through a user interface, which is generally a smart app. The appliances use the smart home gateway as an Internet access point and in some cases they access some cloud services.

3. Threat model and challenges

3.1. Network model

The goal of a security scheme is to allow multiple nodes to communicate in a trustworthy way over an untrusted network. For a smart home scenario, we consider a network that owns a set of devices which offer and use different services in a centralized or a distributed architecture. Each device can communicate with many other devices. The messages exchanged are transmitted over an

[6] https://www.smartthings.com.
[7] https://www.apple.com/ios/home/.
[8] https://getvera.com/controllers/vera3/.
[9] https://nest.com/weave/.
[10] AllSeen members include Qualcomm, Microsoft, LG, Cisco, and AT&T.
[11] https://allseenalliance.org/framework.
[12] https://www.alibaba.com/showroom/smart-living-wireless.html.
[13] https://iot.open.qq.com.
[14] https://www.mi.com/global/list/.

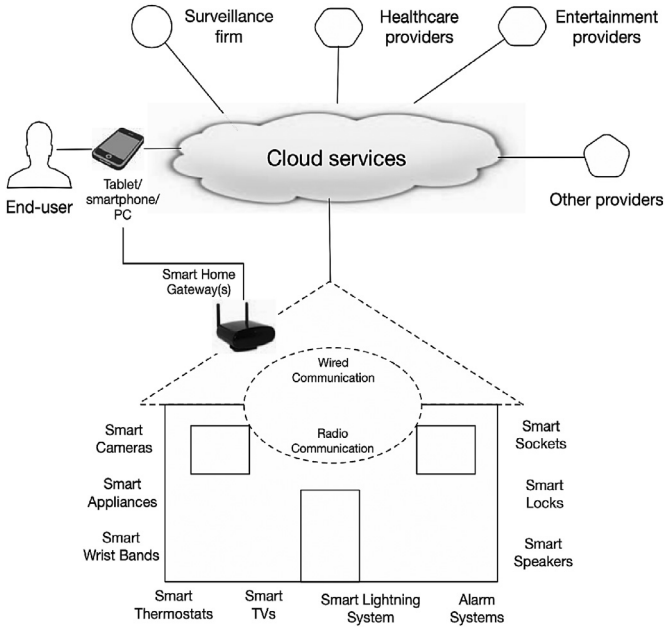

Fig. 3. Generic architecture of current smart home systems from an industry perspective (Bugeja et al., 2016).

unreliable and potentially lossy communication network by using the communication technologies used in smart homes. These communications are performed using: long-range communication technologies such as *Wi-Fi* and cellular technologies, and short-range communication technologies such as *Bluetooth, Zigbee*[15], *Z-Wave*[16], *EnOcean*[17], *Insteon*[18], and *Wavenis*.[19] Some of the smart home services require some devices to access a cloud infrastructure through the Internet. Thus, an Internet access entry point such as a modem/router (commonly called the home Internet box) is required. Moreover, we consider an ecosystem that provides a programming framework for third party developers to build applications in order to provide smart home benefits such as the well-known smart home system namely, the *Samsung's SmartThings* platform. We also assume that all participants cannot be trusted. Indeed, the high number of smart home appliances in the network increases the risk of including compromised ones. Furthermore, the existing devices are of heterogeneous types and do not belong to the same use case. The network function only forwards packets and does not provide any security guarantee such as authentication. Even if some of the communication technologies we have cited earlier use advanced security mechanisms, (e.g., *Zigbee* uses *AES-CCM* for encryption and its *Message Authentication Code* function for authentication and integrity), numerous smart home devices such as sensors and motion detectors cannot apply them due to computation and processing constraints.

More precisely, the network model involves five basic entities, sensing devices, cluster heads, autonomous devices, user devices, and the gateway as the Fig. 4[20] shows.

- The sensing devices are tiny, and the most resource constrained in the device hierarchy. These devices are highly limited in terms of memory, transmission bandwidth, communication range, computational capability, and power capability. Thus, the security operations performed by these devices must be both lightweight and efficient.
- The cluster heads are devices that work as networking hubs that receive data from multiple sensing devices deployed in the network and forward this data to the nearby in range gateway device.
- The user devices host end-user applications which execute user commands.
- The autonomous devices also host end-user applications. However, they work autonomously without human intervention, except for the configuration. They generally depend on a cloud-based application.
- The gateway is a resource capable device that can perform complex cryptographic operations. It receives and forwards data to/from the sensing devices, the user devices, and autonomous devices to/from the Internet (based on the use-case) after completing the verifications and data validation needed. Thus, the gateway device aggregates and forwards the data. For its implementation, two models exist: the uni gateway model and the multi-gateway model. In this work we focus on the uni gateway model as it is the most widely used.

3.2. Attacker model

We assume that an attacker or malicious user has a certain control over the smart home network through a remote attack or physical compromise, i.e., he/she can selectively sniff, drop, replay, reorder, inject, delay, and modify messages arbitrarily with negligible delay. Thus, the devices can receive unaltered and altered messages. However, no assumptions on the rate of the altered messages are made. Besides, the attacker can be equipped with a computation power and storage larger than the implemented devices capacities, in order to execute the attacks efficiently.

3.2.1. Attacks

Cyberattacks can target the different IoT stack layers of the smart home system. The *Open Web Application Security Project (OWASP)* (Rentz, 2019; Team, 2018) considers that weak, guessable, or hardcoded passwords, insecure network services, insecure ecosystem interfaces, lack of secure update mechanism, use of insecure or outdated components, insufficient privacy protection, insecure data transfer and storage, lack of device management, poor physical security, and insecure default settings as the top 10 IoT security vulnerabilities.

The vulnerabilities cited by the *OWASP* can be exploited by a wide range of attacks. Neshenko et al. (2019) proposed a more fine grained classification of vulnerabilities: deficient physical security, insufficient energy harvesting, inadequate authentication, improper encryption, unnecessary open ports, insufficient access control, improper patch management capabilities, weak programming practices, and insufficient audit mechanisms.

An attacker can have multiple goals, such as sending wrong information in order to modify system's decisions or can cause the denial of service of the various devices. The majority of attacks (e.g., message forging, Sybil, and others) and their modus operandi are common to IoT ecosystems. But in a smart home scenario, the goals of attacks and their consequences on humans are quite different. Some of these goals include: (1) Determining the locations of lucrative home burglary targets via camera feeds or the distinctive signatures of multiple, expensive devices (Denning et al., 2013), (2) Checking whether or not a home is occupied (and by whom) via cameras, microphones, motion sensors, logs for lights, thermostats, and door locks, Heating, Ventilation and Air-Conditioning (HVAC),

[15] https://www.zigbee.org.
[16] https://z-wavealliance.org.
[17] https://www.enocean.com.
[18] https://www.insteon.com.
[19] http://www-coronis-com.dyn.elster.com/downloads/Wavenis_Data_Sheet_A4_CS5.pdf.
[20] The user interface (e.g., a smart app) can communicate with some of the devices through the local network and through the Internet.

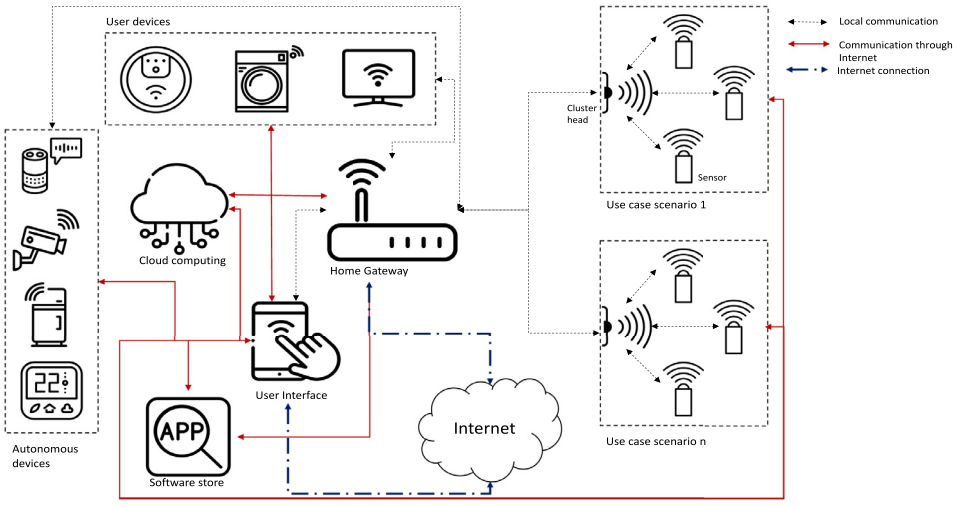

Fig. 4. Network model for a smart home.

air pressure sensors, (3) Remotely manipulating a washing machine to cause flooding, (4) Targeting entire communities by coordinating their devices to overload the power grid (Denning et al., 2013), (5) remotely controlling faucets in order to waste water and cause financial harm, or (6) eavesdropping video or conversation records that may contain private content about the intimacy and private life for extortion purposes. Thus, we describe these attacks with a special focus on their consequences on a smart home ecosystem.

(1) Default/hardcoded passwords: currently, there exist multiple advanced authentication methods that rely on reliable and robust cryptographic algorithms (El-Hajj et al., 2019; Zeadally et al., 2021) such as those that rely on IoT-adapted Transport Layer Security (TLS) or Datagram Transport Layer Security (DTLS) (Tiburski et al., 2017; Urien, 2015), One Time Password (OTP) (Hammi et al., 2020) and many others. However, for reasons of practicality, quality of service, and devices' constraints, minimal and more intuitive security mechanisms are used. Additionally, the username/password technique is the most predominant. Even worse, because of the lack of consumers' sensitivity to cybersecurity issues, most of them do not even modify the default username/password when they deploy these devices. In other cases, the devices are provided with hardcoded credentials, that cannot be modified by the users, even if they wish to do so.

Default and hard coded passwords represent one of the main security issues in IoT and smart home systems (Singh Verma and Chandavarkar, 2019). Indeed, when consumers buy smart home products, they are often set up with default or hardcoded credentials, generally in the form of a username and a password. These credentials are often available on the vendor's website and are frequently easily guessable, which facilitate unauthorized access to IoT devices and home network via different cyberattacks such as data identity theft, social engineering, access to IoT cshell service (reverse shell), insecure web services and more (Singh Verma and Chandavarkar, 2019). It also allows malware such as *Mirai* (Marzano et al., 2018) to compromise home devices and exploit them for data exfiltration or to execute various attacks such as buffer overflows, Structured Query Language (SQL) injection, Remote Code Execution (RCE), remote code injection, Distributed Denial of Service (DDoS), and so on Hamad et al. (2020).

For example, the password management company *SplashData* evaluated more than five million passwords leaked on the Internet during the previous years and compiled the top 100 worst passwords for 2018. Surprisingly, for the fifth straight year, the top spots (#1 and #2) in the annual worst-of-the-worst list remain unchanged: "123456" and "password" (Rentz, January 2019; Wor, 2020).

(2) Malware/botnet: In the last few years, malware developers' have shown increasing interests in IoT devices. For example, the *Mirai, Bashlite* and *Silex* malware all aimed at IoT and smart home devices. *Bashlite*, also called *Gafgyt*, which is considered as *Mirais* predecessor exploited vulnerable IoT devices that used weak or default credentials (Marzano et al., 2018). More precisely, it exploited the *CVE-2017-5638*[21] *Apache Struts vulnerability* (Osborne, 2018). However, *Mirai* was much more sophisticated than *Bashlite*. Indeed, according to Gopal et al. (2018) as *Bashlite, Mirai* relies on default username and passwords from vulnerable devices to attempt brute force attacks and further add these devices to the botnet army. Every bot that *Mirai* obtained, it would scan for nearby vulnerable devices and report back to the Command and Control server (C&C). *Mirai* is one of the most well-known botnet malware types because it was the source of the largest Distributed Denial of Service (DDoS) attack in history that reached a throughput of more than 1.7 Terabytes/second in 2018 (Antonakakis et al., 2017; Kambourakis et al., 2017; Kolias et al., 2017; Seralathan et al., 2018).

When a device is infected by *Mirai*, it disseminates the malware by scanning other random public addresses searching for TCP ports 23 or 2323. Then, it attempts the following steps (Wells, 2020): (1) It executes a brute force attack on the scanned devices relying on a small dictionary of 62 possible username/password pairs that are common to IoT devices, (2) If the brute force is successful, it sends an administrative shell to the infected system and reports back to the report server using a different port. Meanwhile, the C&C server continuously scans for potential victims, (3) The botmaster issues an infect command which payload contains information such as IP address and hardware architecture, (4) The payload then logs into the infected device and instructs it to download and execute the corresponding binary version of malware. In addition, *Mirai* looks for any other type of malware and closes points of entry like Telnet and Secure Shell (SSH) services.

The efficiency of *Mirai* has increased the appetite of cyber criminals and variants of *Mirai* are discovered continuously. For example, the *Mukashi* botnet is a variant of *Mirai* that exploits the *CVE-2020-9024*[22] on *Zyxel* Network Attached Storage (NAS) devices

[21] https://nvd.nist.gov/vuln/detail/CVE-2017-5638.
[22] https://nvd.nist.gov/vuln/detail/CVE-2020-9024.

running firmware version 5.2.1 in order to gain access and take control of the targeted devices (Ken et al., 2019). According to Palmer (2020) the *Mukashi* malware scans TCP ports for potential services running on devices to execute a brute forcing attack to bypass default credentials since March 12, 2020.

The easiness of the brute force attack to access IoT devices enables hackers to create large botnets quickly instead of waiting several months as it is the case for traditional botnets (Hammi et al., 2019). For example, a hacker called *Anarchy* enslaved 18,000 devices in only 24 hours by exploiting the *CVE-2017-17215*[23] vulnerability from which suffered *Huawei* routers and smart home devices (Osborne, 2018). Another consequence of this brute force easiness, is the increase in the number of devices' infections. Indeed, *Kaspersky Labs* stated that they identified 24,610,126 unique malicious objects in 2019, 14% more than they identified the previous year (Kaspersky, 2020). Also, according to *Malwarebytes labs* (Labs, 2020a), a 42% increase in the category of hack tools was detected.

IoT botnets provide more options and advantages to cyber criminals and allow them to execute more severe attacks. For example, in 2016, hackers realized the biggest DDoS attack in history using *Mirai* botnet. *LizardStresser* is another example of an IoT based botnet that uses default credentials to brute force devices and convert them into bots. It was used to launch 400 Gbps attacks against targets such as the *British Broadcasting Corporation (BBC)*, two large Brazilian banks, two Brazilian telecommunications providers, two Brazilian government agencies and three large gaming companies in the United States (Osborne, 2016). IoT based botnets are not limited to DDoS attacks. Indeed, a security team at *Proofpoint* discovered a botnet which specializes in infecting home appliances, especially televisions, routers, and fridges. The botnet involved over 100,000 devices that were used to send at least 750,000 spam and malicious emails (Proofpoint, 2014a; 2014b). Here again, the home appliances were controlled through mis-configuration and the use of default passwords (Osborne, 2014).

Silex is another example of malware which runs on the Internet with a focus on rendering IoT devices inoperable. *Silex* focuses on Unix-based devices with default username and passwords (Hamad et al., 2020). When *Silex* finds a vulnerable device, it overwrites all of the systems storage with random data, wipes out the firewall rules and network configuration, and then restarts the system making the device inoperable to consumers (O'Donnell, 2019; Wells, 2020). It is reported (Cimpanu, 2019) that this destructive malware was created by a 14-year-old teenager. *Silex* affected up to 4000 vulnerable IoT devices before the creator shut down the command and control server.

(3) Denial of Service: Compromised home appliances can be used to launch Denial of Service attacks against targets over the Internet. But these appliances can also be the target of such attacks. A Denial of Service (DoS) or a Distributed DoS (DDoS) attack is characterized by the explicit attempt by the attacker to prevent the legitimate use of a service. There are two methods to conduct a DoS/DDoS attack (1) by exploiting a protocol flaw and (2) by flooding the target. DDoS and especially flooding attacks are among the most dangerous cyber attacks (Badis et al., 2014) and their popularity is due to their high effectiveness against any type of service because they do not require identification and exploitation of protocols' or services' flaws, but only need to flood them (Hammi et al., 2014), which can be easily executed due to the limited memory and processing capacity of the smart home devices. In the smart home context, numerous DoS/DDoS scenarios are possible on the home's devices to prevent them from performing their tasks such as sensing, monitoring or processing. In this case, the consequences of the attack can vary. Indeed, a DoS attack that targets a motion sensor has a different consequence from a DoS attack that targets a smart fridge leading to food waste, which in turn have different consequences from a DoS/DDoS attack that targets a healthcare system, that can have disastrous consequences on the patient's life (Denning et al., 2013). However, in some cases, the DoS/DDoS attack can paralyze the whole smart home system. Such cases include: (1) a DoS/DDoS on the C&C unit (in the case of a centralized architecture), (2) a DoS/DDoS attack that targets the Internet box which paralyzes all services (such as cloud-based applications) that rely on the Internet, and (3) a DoS/DDoS attack that targets the grid's smart meter which cuts off electricity in the house which in turn disables all the services provided by the majority of devices.

(4) Scanning attack: Each cyberattack requires different phases. One of the most important phases is the identification of the potential victims which is achieved through scanning. Unfortunately, it is easier for the hackers to find vulnerable IoT devices than other non-IoT targets by diverting the use of existing tools. Indeed, there are different vulnerability scanning tools such as *Zmap*[24] or *Censys*[25], and other online tools such as *Thingful*[26] that are used for gathering data from connected machines and IoT devices, but *Shodan*[27] is currently the best due to the ease of use of its web interface and Application Programming Interface (API) (Fernández-Caramés and Fraga-Lamas, 2020; Genge and Enăchescu, 2016).

Shodan (Matherly, 2016) is one of the most popular search engines available today, designed to crawl the Internet and to index discovered services (Genge and Enăchescu, 2016). Thus, it includes information about systems and devices publicly facing the Internet. With different types and categories of search queries, users can extract information about those systems/devices. In many cases, users of those systems may not be aware of the amount of information that is publicly exposed about their systems. Those systems are usually installed according to the manufacturers installation manuals, and in many cases, users may keep default settings designed by manufacturers (Albataineh and Alsmadi, 2019; Matherly, 2016). For example, researchers from *Bitdefender* used *Shodan* to detect more than 100,000 Internet-connected security cameras that contain a "massive" security vulnerability that allows them to be accessed via the open web and used for surveillance, roped into a malicious botnet, or even exploited to hijack other devices on the same network (Bitdefender, 2015; Bugeja et al., 2018). Two cameras manufactured by *Shenzhen Neo Electronics*, China, were found to permit attacks without even logging into the system to gain unauthorized access (Bitdefender, 2015).

(5) Compromised/over-privileged applications: as we have described earlier, there are new frameworks for third-party developers to build applications that interact with the smart home devices. These frameworks provide tangible benefits to their users, but, also expose users to significant security risks (Fernandes et al., 2016): (1) If the user sets up a compromised application developed by a malicious user and made it available on the applications' store, the attacker can get any data obtainable by the devices that use the application or by the devices allowed to cooperate with the device running the application. (2) In numerous cases, the installed application is developed by some honest peer, nonetheless, it requests more privilege than it needs, which considerably increases the attack surface, weakens the system and provides a source of information to any malicious user who physically compromises a smart home device that runs the application or just by communicating with it. In this context, *Fernandes* et al.proposed an empiri-

[23] https://nvd.nist.gov/vuln/detail/CVE-2017-17215.

[24] https://zmap.io.

[25] https://censys.io.

[26] https://www.thingful.net.

[27] https://www.shodan.io.

cal security evaluation of *SmartThings* framework. They discovered that over than 55% of existing *SmartApps* did not use all the rights that they initially requested when they were installed; *SmartThings* grants a *SmartApp* full access to a device even if it only requires limited access; and the *SmartThings* event subsystem has inadequate security controls (Fernandes et al., 2016).

(6) Message forging or substitution Attack: in a substitution attack, the attacker intercepts valid messages during their transit and alter them in such a way that recipients accept the forged messages as if they had been sent by the original sender. The attacker can also just forge a new message and sends it to the victim. This attack can have disastrous consequences in some scenarios such as healthcare by tampering with the devices in order to change treatments or notifications. Moreover, this attack can be used to remotely control devices such as (1) controlling the locks in order to open or close doors (for burglary purpose), (2) manipulating the settings of thermostats and heating systems to waste energy for increasing energy bills causing financial harm, (3) issuing false carbon monoxide alarms, (4) disable holidays mode or disabling the surveillance system for burglary purposes.

The False Data Injection (FDI) attack is a well-known in the smart grid environment (Kubo, 2018) and its impact and damages have been extensively studied (Liang et al., 2016; Liu et al., 2015; Musleh et al., 2019; Ünal et al., 2021). However, in this paper we are interested in FDI attacks on smart grid from a smart home perspective. In this case, the FDI attack targets the home's smart meter (node of the smart grid). In an FDI attack, the attacker aims to inject malicious measurements to mislead the state estimation process (Liang et al., 2016). Musleh et al. (2019) classified the impacts of FDI attacks in smart grids into financial impact and stability impact. In the case of financial impact, in the smart home context, we can distinguish two attacker profiles; (1) the smart home's owner is the victim, where an attacker substitutes/injects the messages that the smart meter sends to the grid transmission center to transmit false information of house's consumption, in order to increase the energy bill and cause a financial harm. (2) the smart home's owner is the attacker and injects false data to mislead the operator about the home's energy consumption in order to achieve a financial gain by not paying the real amount owed.

There are various examples of the stability impact of FDI. Chen et al. (2016) demonstrated how a coordinated FDI attack could lead to an unnecessary generation rescheduling and load shedding. Konstantinou et al. (2017) showed how an FDI attack on the GPS signal could lead to a major load shedding. Wu et al. (2017) illustrated how a simple FDI attack could propagate and lead to a full blackout. ***(7) Message replay attack:*** an attacker can selectively record some messages and replay them without modification at a later time because the successful verification of a message does not certify the correctness of the message's sending time. In this way, inaccurate information can be intentionally provided to the devices or to the servers. Message replay attack is usually combined with a message removal attack and is deployed when signature-authentication is used to accept the messages. It can be used to achieve the same goals discussed in the latter attack (message forging or substitution attack).

(8) Sybil attack: the Sybil attack is described as a malicious node taking on multiple identities illegitimately (Can and Sahingoz, 2015). Hence, in multiple cooperative use cases, the attacker simulates the existence of multiple entities (devices) that send wrong information to the service's decision unit or management application in order to perform actions (following an election process) the attacker wants. For example, an attacker can generate numerous fake messages coming from fire sensors to make believe that a fire is occurring throughout the house. The same scenario is possible by tampering with the different carbon monoxide devices in the house.

(9) Spoofing attack: in contrast to the Sybil attack where the attacker try to create numerous false or virtual identities, in the case of a spoofing attack, the attacker tries to spoof the identity of a legitimate user in order to make use of his/her privileges.

(10) Eavesdropping: is an attack where an adversary can choose to passively eavesdrop on the network communication and steal the data. Traditional encryption techniques cannot be applied in numerous cases because of the various technical constraints of the smart home devices. Thus, an attacker can access different types of data such as cameras video records (generally, video records are stored for a pre-determined period of time) during their transmission to the storage server. The attacker can also access some sensitive data (such as banking information (e.g., credit cards numbers) stored by some devices for ordering purposes) if it is not well protected.

(11) Physical node compromise: it represents the act by which a legitimate node in the home's network is captured and compromised, that is, reprogrammed by an adversary. Hence, a compromised node running malicious code disguised as a legitimate node can be used to launch any insider attack.

(12) Adversarial machine learning: Artificial intelligence techniques and especially machine learning are vital to the development of the smart home environment. Indeed, all the autonomous home appliances rely on such techniques. Furthermore, multiple research works have proved that machine learning is among the most effective techniques that can help in attack and intrusion detection (da Costa et al., 2019; Din et al., 2019; Zeadally et al., 2020). However, machine learning algorithms are vulnerable to various types of attacks such as membership inference attacks (Shokri et al., 2017) and evasion attacks (Biggio et al., 2013). However, the most common attack is adversarial machine learning (Huang et al., 2011; Kurakin et al., 2016; Vorobeychik and Kantarcioglu, 2018). That is, legitimate inputs altered by adding small, often imperceptible, perturbations to force a learned classifier to misclassify the resulting adversarial inputs, while remaining correctly classified by a human observer (Papernot et al., 2017).

In the smart home context, we classify adversarial machine learning into two categories:

(1) Attacks against home appliances: as described, autonomous home appliances rely heavily on machine learning. Adversarial machine learning is known to be very effective against systems that treat data related to image or speech processing (Papernot et al., 2017). Image and speech processing techniques are commonly used in smart home appliances (e.g., face recognition, camera assisted appliances (smart vacuum), voice assisted appliances (smart personal assistant), and so on). These attacks can also target other autonomous systems (e.g., autonomous healthcare systems)[28]. Therefore, an attack against these systems can cause various damages to the smart home ecosystem, ranging from manipulation of devices and appliances to full disruption or even severe or even fatal injuries to the home residents.

(2) Attacks against home intrusion detection systems: adversaries can use the aforementioned attacks to not only disrupt system's activity but also to achieve evasion by causing the intrusion detection system to have many false negatives. Indeed, as described above, intrusion detection systems that rely on machine learning are among the most effective and are widely used today. Therefore, an attack against such system can lead to disastrous consequences to the smart home environment. For example, Huang et al. (2011) showed that, by injecting crafty chaff into the network during training, the detector can be poisoned rendering it is unable to effectively detect DoS attacks. Relying on the same method they could launch an attack against a spam filter and

[28] https://autonomoushealthcare.com/.

were able to pass spam emails through it. In the same context Xu et al. could launch an attack where a malware was identified as legitimate (Xu et al., 2016b).

3.2.2. Discussion

Numerous studies show that the majority of homeowners remain oblivious to the cyber threats associated with IoT connected devices and fail to educate themselves on available security options to prevent or mitigate such threats (Wells, 2020). As it was discussed, one of the major security issues is the default configuration/credentials that are not modified by users after the devices have been deployed. This can open the door to multiple kinds of attacks. The most virulent one remains the malware infection. As discussed, the majority of malware programs such as *Mirai, Bashlite, Mukashi* and many others rely on default and hard coded credentials to get access to devices (Singh Verma and Chandavarkar, 2019).

Once a device is infected, it allows the hacker to use it as a bot (for DDoS, spam or other attacks) or to use it to reach and hack other parts of the home network, especially that home networks are not that secured. Indeed, according to a study made by *Verizon* (Verizon, 2020), 70% of Wi-Fi sessions were over unencrypted networks, yet only 50% of survey respondents had a solution for encryption. This creates significant security risks for attack such as passive attacks (e.g., man in the middle). Another study made by *Netsecurity* (Security, February 2020) found that 83% of IoT devices communicate over insecure channels. They examined 553 different IoT devices across 21 categories from 212 manufacturers. Out of the 553 different IoT devices, the top unauthorized devices include digital home assistants, TV set-top boxes, IP cameras, smart home devices, smart TVs, smart watches, and even automotive multimedia system.

Studies (Labs, 2020a; Wells, 2020) agree that the sophistication of malware has evolved, with the use of exploits, credential-stealing tools and multi-stage attacks resulting in mass infections of an attackers target. A single threat in a network poses a significant risk to the entire network. IoT threats are not only directed at devices. For instance, threats can be directed at people, machinery, devices, systems, services, software and more. No one can predict what type of threats consumers will emerge in coming years, however, future threats are anticipated to be more extensive and dangerous than today (Sahinaslan, 2019; Wells, 2020).

The ignorance/negligence of consumers is just part of the problem. Some devices contain hard coded credentials that are not possible to modify by consumers. These default hard coded credentials are often posted by vendors and manufacturers on their websites, which give attackers an advantage when making malware. Moreover, with the emphasis on production, cost, size and usability, manufacturers and other IoT vendors, frequently give security concerns a lower importance, with many ignoring it altogether (Stoyanova et al., 2020). It is also worth noting that implementing efficient security mechanisms is a very hard task in constrained devices.

Alrawi et al. (2019) conclude that there are three main attack vectors in relation to IoT devices and smart home systems: vulnerable services, weak authentication, and default configurations. Unfortunately, it is very easy to find vulnerable smart home devices using tools such as *Shodan, Thingful* or others. Indeed, the latter are able to find consumer's home devices with weak security control such as medical devices, cameras, systems, environmental controls and more. *Shodan* can be used for vulnerability and penetration testing assessments alongside with *Google Hacking Database (GHDB)*[29] (Genge and Enăchescu, 2016; Wells, 2020).

In a smart home scenario, the goals of attacks and their consequences on humans are quite different. Next, we describe some of the numerous attacks that occurred. In December 2019 parents of three daughters installed *Ring* cameras in their bedrooms in order to have an extra set of eyes. However, because the parents did not change the default credential, a hacker could get access to the home network and took the control of a wireless speaker. Using the camera's video flow and the smart speaker, the attacker harassed their little 8 year old girl[30]. In the same context, a Milwaukee couple was left feeling violated after their home camera began talking to them, their thermostat suspiciously topped 90 degrees and vulgar music blasted through their wireless electronics.[31]

A security breach can lead to many other security/privacy breaches. For instance, a team of hackers recently discovered a man-in-the-middle vulnerability in a *Samsung* smart refrigerator that can be exploited to steal *Gmail* users' login credentials.[32] In the same context, *Check Point Research* (Labs, 2020b) discovered another attack that makes it possible for a rogue *Hue Philips* light bulb to hijack the *Philips Hue* bridge. *Philips Hue* Bridge is the C&C of smart lighting systems which allows to connect and to control lights and accessories. The latter system uses *ZigBee* protocol for communication. A vulnerability in the *ZigBee* protocol allowed hackers to exploit it by taking control of a *Hue Philips* light bulb and turning it on and off, as well as controlling its color or brightness to trick users into thinking the bulb has a glitch. The bulb appears as Unreachable in the users control app, so they will try to reset it. The only way to reset the bulb is to delete it from the app, and then instruct the control bridge to re-discover the bulb. The bridge discovers the compromised bulb, and the user adds it back onto their network. The controlled bulb with updated firmware then uses the *ZigBee* protocol vulnerabilities to trigger a heap-based buffer overflow on the control bridge, by sending a large amount of data to it. This data also enables the hacker to install malware on the bridge, which is in turn connected to the target business or home network. The malware connects back to the hacker and using a known exploit such as *EternalBlue*, they can infiltrate the target IP network from the bridge to spread other malware programs (Labs, 2020b). The bad news about this attack is that, in 2016, Ronen et al. (2017) launched an attack using drones to take control of *Philips Hue* light. It was stated that the same vulnerability from the 2016 attack was used to discover the latest exploit in 2020 (Labs, 2020b).

Another example of the consequences of security issues on home appliances relates to attacks on smart meters (He et al., 2017; Zeadally et al., 2013). Indeed, smart meters are generally connected to all home devices. Unfortunately, they have generally the same manufacturer access credentials, which make them among the first choice targets of hackers as stated by a *Federal Bureau of Investigation (FBI)* Report.[33] According to the researcher *Netanel Rubin*[34], security problems of smart meters can lead to disastrous consequences because hackers could turn a smart meter into a bomb to cause explosion and start a fire.

Smart home appliances generally rely heavily on cloud computing, and attacks on the latter (e.g., DoS) can disturb the operations of smart home appliances. For example, in 2017 an outage at cloud

[29] https://www.exploit-db.com/google-hacking-database.

[30] https://www.nytimes.com/2019/12/15/us/Hacked-ring-home-security-cameras.html.

[31] https://www.foxbusiness.com/technology/smart-home-virtual-intrusion.

[32] https://www.theregister.com/2015/08/24/smart_fridge_security_fubar/.

[33] https://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/comment-page-1/.

[34] https://www.youtube.com/watch?v=k2EpY3-kDww.

provider *Amazon Web Service (AWS)*, left numerous consumers that use smart lighting systems literally in the dark for many hours.[35]

Physical security and system services are not the only vulnerabilities adversaries can exploit. Protocols created specifically for IoT devices have their own issues that can be exploited to take control of IoT devices (Das et al., 2018; Wells, 2020; Zeadally et al., 2021). *Zigbee* is one of the most vulnerable protocols. For example, in *Zigbee 3.0*, it was found that the preinstalled master keys used by *Zigbee Alliance* were leaked in 2015, which made thousands of devices that rely on it vulnerable to cyberattacks (Krejčí et al., 2017). Moreover, the keys did not expire which means that adversaries could reuse the keystream for however long they desire. Another example is the implementation flaw in *Zigbee* stack in *Atmel* chips used by *Phillips Hue*. The security breach can allow an adversary to reset a device to factory settings and allow consumer IoT devices to connect to the attackers network. Devices that use *Zigbee* are also prone to DoS attacks. One of the ways to achieve a DoS attack on a *Zigbee* device is through the Ghost-in-Zigbee attack which performs a DoS attack via energy depletion. This attack takes advantage of the payload encryption in IEEE 802.15.4. Since the device address and counter value are unencrypted, an adversary can generate messages for any *Zigbee* capable device. If the integrity check fails and the message is unused, it will eventually lead to battery depletion and DoS attack on the device (Cao et al., 2016; Krejčí et al., 2017).

Smart TVs are among the weakest links in a smart home scenario, especially when many of the new TVs are equipped with built-in cameras. Indeed, according to an *FBI* release smart TVs can be the gateway for hackers to gain access to a home network. Additionally, they can be used to put backdoors in home routers, take control of the TV, change channels, change volume level, and more (FBI, 2019; Wells, 2020). According to *Vault7*[36], the *Central Intelligence Agency (CIA)* created a program in order to monitor users by exploiting vulnerabilities in *Samsung* smart TVs (Park et al., 2019c).

Fig. 5 depicts a detailed taxonomy of the cyber attacks and threats for smart home environments that we identified in the literature. Some of them have been discussed earlier in this section. It also shows a classification of the security requirements and challenges for the smart home ecosystem, that we identified from the different related works. We discuss them in the next section.

3.3. Security and safety requirements and challenges

As a result of the rapid growth of smart home appliances and devices, the number of potential attackers and the size of IoT networks are growing exponentially. Thus, a smart home ecosystem must fulfill several security requirements and face multiple challenges in order to ensure its sustainability and resiliency.

According to Herrmann (2007), safety is the feature that ensures that a device performs predictably under normal and abnormal conditions and the likelihood of an unplanned event occurring is minimized and its consequences controlled and contained. We define security as the feature that prevents devices from unwanted or illegal activity. In other words, safety ensures the reliability of a given system while security ensures its protection against cyberattacks. Next, we discuss several security and safety requirements for smart homes.

(1) Privacy: privacy is an important requirement in the smart home's ecosystem. However, it remains a very hard challenge to achieve. The number of connected devices in the home is growing exponentially. These Internet-connected devices can sense and record every aspect of the resident's life, generally without his/her knowledge, even during the most intimate moments. For example, a sex toy company has admitted that its products have been secretly recording users' intimate sessions.[37] Moreover, the emergence of the paradigm of Social IoT (SIoT) (Atzori et al., 2012; Mohammadi et al., 2019) makes privacy protection even more challenging. In such a context, devices such as personal assistants communicate with the users and provide services such as web browsing, shopping, tweeting, reading/sending emails, news, messaging, providing calls, and so on. Many consumer devices use on-device keyword spotting that triggers devices with microphones to record and upload audio to the Internet. Smart assistants, for instance, listen for a keyword (e.g., Alexa) or a key phrase (e.g., Hey Siri). Once they hear the keyword or phrase, they start recording and send the recording to server-side components. In the case of compromised or over-privileged applications, microphones and cameras, data exfiltration can be triggered without a keyword spotting mechanism.

In the case where the user accepted, without really being aware of the privacy policies of the device, its data will be used in various types of profiling including targeting advertisements or commercial/political manipulations. Worse still, if the resident uses a compromised device it can be used for extortion following the recovering of intimate videos or discussions. Moreover, the failure of devices can always occur, leading to potential privacy exposure. For example, the *Amazon Echo* device recorded a family's conversation and emailed it to a seemingly random person on their contact list[38].

According to a research conducted by *Palo Alto* (U. 42, 2020), 98% of all IoT device traffic is unencrypted which exposes personal and confidential information over the network allowing adversaries the ability to listen to unencrypted traffic and use the data to profit on the dark web. Additionally, 57% of IoT devices were found to be vulnerable to medium or high severity attacks making them low hanging fruits for attackers. Furthermore, about 41% of vulnerable IoT devices get exploited through network-connected devices to exploit known weaknesses. These IoT devices were often used in lateral movements to search for more devices to attack (Wells, 2020).

(2) Interoperability: interoperability is one of the biggest challenges for smart home development. Currently, devices cannot fully cooperate and understand each other because of two main reasons: (1) technical non-interoperability of respective protocols. There exist some solutions to address this issue. For example, there are numerous products that ensure a communication gateway between the different networking protocols[39] [40]. However, relying on a gateway could add communication delays, which can have consequences on real-time systems. (2) Industrial/commercial competition in order to be the leader of the smart homes market, leading the products' developers to intentionally encourage non-interoperability between their devices and competitive products from other vendors. For example, *Google* devices are incompatible with *Apple* devices.

Interoperability issues can open up numerous security problems. Indeed, IoT devices use various technologies, protocol, and standards such as *Bluetooth, Zigbee*, Domain Name Service (DNS) and more are utilized by multiple devices and vendors. In other words, home security automation systems are built using different devices from different manufacturers. For this reason, IoT systems are more susceptible to security breaches (Chitnis et al., 2016).

[35] https://www.theguardian.com/technology/2017/mar/01/amazon-web-services-outage-smart-homes.

[36] https://www.wikileaks.org/vault7/.

[37] https://www.theverge.com/2017/11/10/16634442/lovense-sex-toy-spy-surveillance.

[38] https://www.darkreading.com/iot/spies-among-us-tracking-iot-and-the-truly-inside-threat/a/d-id/1333015.

[39] https://www.silabs.com/products/development-tools/wireless/mesh-networking/z-wave/z-ip-gateway.

[40] https://www.hackster.io/ThereIsNoTry/insteon-gateway-eaef24.

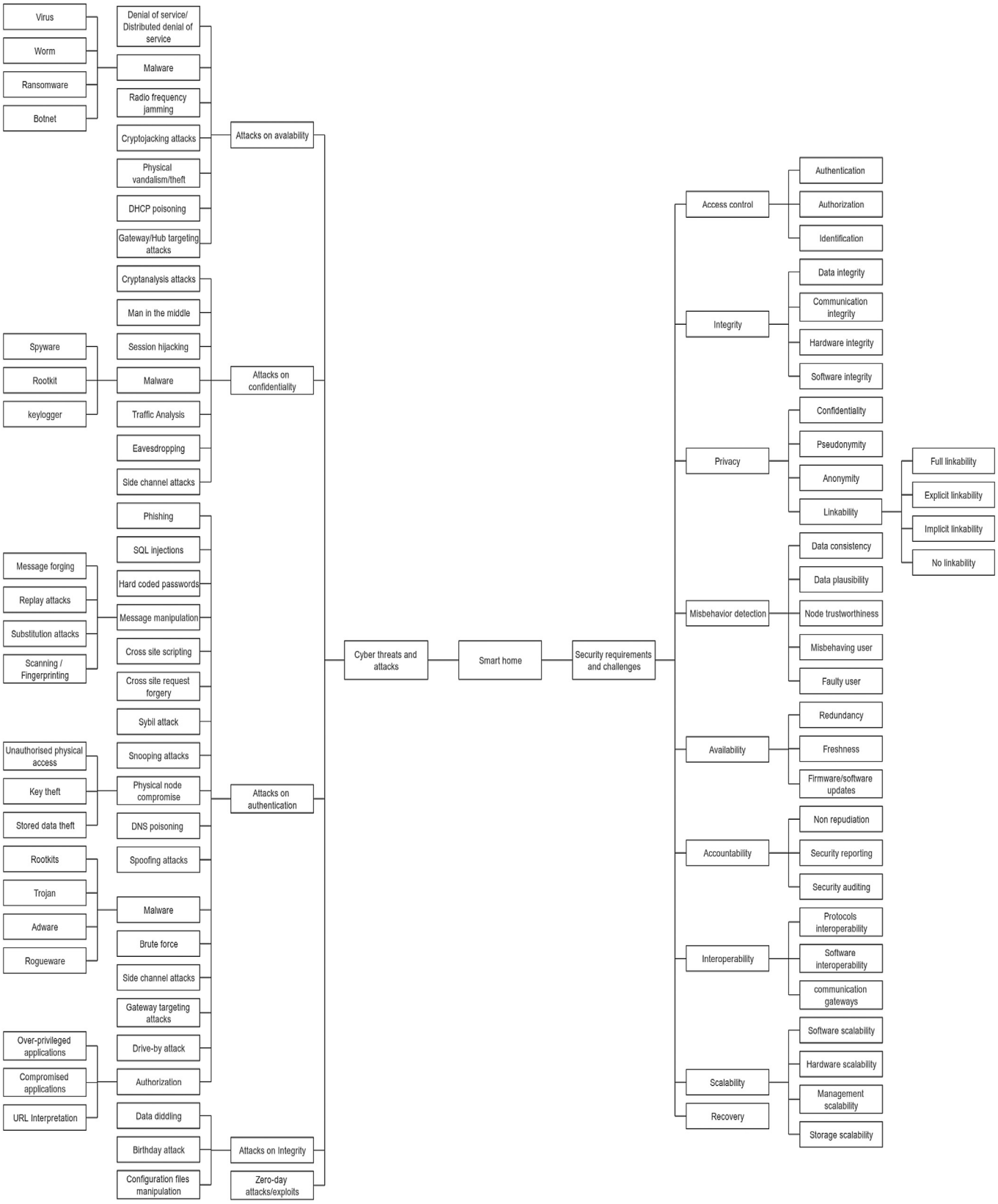

Fig. 5. Taxonomy for security requirements, challenges and cyberattacks for smart home environments.

(3) Security of routers: home routers are the most exposed devices to cyberattacks. Besides, in most cases, they represent the entry point to hack the other home devices which makes them a first choice target for hackers. For example, according to the *FBI* (FBI, 2018) there is a security threat posed to home routers by attackers using *VPNFilter* malware, which had the capability to block network traffic, collect information and exploit other connected devices. Another study made by *TechRepublic* (Jason et al., 2017) states that tens of thousands of Wi-Fi routers are potentially vulnerable to an updated form of malware that takes advantage of known vulnerabilities to rope devices into a botnet. The *Bashlite* malware could affect three different wireless router models: *Huawei HG532, Realtek RTL81XX*, and *Zyxel P660HN-T1A*.

Enterprises' routers are generally well secured because they are deployed by experts. However, home routers are generally deployed by consumers who are generally ignorant of security issues, which makes these home routers vulnerable to numerous attacks. Indeed, according to an *Avast* study (Nunziati, 2018) 51% of owners have never logged into their routers administration page, and 72% never updated their routers firmware.

(4) Identification: this is a major requirement in most smart home use cases. It represents the opposite of the anonymity which ensures that any entity can make use of the system while being anonymous to all entities in the system (Hammi et al., 2018). For example, if a motion sensor indicates that all persons have left a room in order stop its heater, the control entity must know exactly which sensor have sent the information to issue the appropriate command to the right heater.

(5) Authentication/mutual authentication: authentication is the mechanism of proving identity. Mutual authentication requires both communicating parties to authenticate each other. This requirement is necessary to protect the system against spoofing the roles of entities. For example, in the smart heating scenario, the command and control entity must authenticate the information sent by the thermostat which must authenticate the control entity to execute its commands.

One of the reoccurring attack vectors for gaining access to IoT devices are insecure authentication and authorization implementations. For example, IoT systems rely on authentication implemented by protocols such as Brick, Data Distribution Service (DDS), *Zigbee, ZWave, Bluetooth Low Energy (BLE)*, and others.

(6) Pseudonymity: this is the mechanism of not using the real device's identifier for communication, but using a pseudonym instead. In such systems, legitimate devices can know if a pseudonym belongs to another legitimate device or not. Pseudonymity can face numerous attacks such as spoofing, messages' forging or substitution. For example, in the Cooperative Intelligent Transportation Systems (C-ITS) context, each station uses simultaneously two certificates provided by a Public Key Infrastructure (PKI): (1) an Enrollment Certificate (EC) and (2) a Pseudonym Certificate (PC). Known only by the EC Authority (ECA) and its owner (the station), the EC is not used in common communications, but used only to authenticate the station to the PKI in order to request new PCs. However, the PC is used for the station's communications (Monteuuis et al., 2017). To protect the privacy of the road users, pseudonyms should be changed frequently. As for the C-ITS use case, generally, this requirement is ensured through public key infrastructures. However, due to smart home's devices constraints, applying such schemes may not be appropriate. Thus, new pseudonymity schemes must be developed.

(7) Integrity: Maintaining integrity is a crucial requirement that each smart home scheme must ensure. Integrity in networks is ensured through error detection and correction schemes such as the Cyclic Redundancy Check (CRC), Parity bit, checksum and so on. Unfortunately, such schemes are not resilient because they can be manipulated easily by an attacker. To address this weakness, cryptographic error detection schemes such as hash functions or Message Authentication Codes (MAC) can be deployed.

In our context, integrity is divided into two parts: (1) Messages (transactions/communications) integrity: an exchanged message must not be altered or modified during its transmission over the network. However, the most popular protocols do not implement integrity-resilient mechanisms. For example, *Z-Wave* uses the header checksum mechanism, *EnOcean, Wavenis* and *Insteon* uses the *Cyclic Redundancy Check (CRC)* mechanism and *X10* does not use an integrity check mechanism.[41] Even when some protocols (such as *Zigbee*) implement resilient cryptography-based mechanisms to ensure integrity, such mechanisms cannot be applied to all existing smart home IoT devices due to their technical design constraints. (2) Data integrity: involves maintaining the consistency and trustworthiness of data over its entire life cycle. Thus, only authorized users can modify stored data (e.g., a system's parameters).

(8) Lack of qualified administrators: smart home appliances are generally setup by householders. The latter usually lack of experience in setting up IT systems and (1) may not install them correctly which increases attack surface or (2) just may not apply best practices such as changing passwords. Thus, a malicious user can easily access connected devices by using default password available on devices' user manual as it was demonstrated by *Avast* research described earlier.

(9) Scalability: in our context, scalability represents the ability that ensures that the system's size has no impact on its performances. For example, if the number of appliances in use grows exponentially, the time needed for a system function must not be affected.

(10) Non-repudiation: It refers to the ability to ensure that an entity cannot deny having performed a given action (e.g., the C&C cannot deny having sent a command to a heater).

(11) Firmware/Software update: There is a real difficulty in updating IoT devices currently in use throughout the millions of homes across the world (Zou, 2019). Sometimes these devices may cause service disruption and, in some cases, can break the device if done improperly (Wells, 2020). Worse still, numerous devices do not have the capability to receive updates. Finally, there is no one-size-fits-all approach in relation to IoT devices which makes update tasks of these devices challenging.

4. Countermeasures and recommendations

4.1. Existing works

There are numerous works (Ali and Awad, 2018; Alrawi et al., 2019) that have proposed security solutions for smart homes. In this section, we propose a classification of these works. We selected these specific works based on their relevance while surveying the maximum number of recent works at the same time.

1) Surveillance/Alarm systems: Surantha and Wicaksono (2018), proposed a system to monitor the presence of an intruder in the house by using combination of motion detection and object recognition. The motion detection is performed using Passive InfraRed (PIR) sensors. After the motion of object is detected, the web camera takes the picture of the suspicious spot. The system then performs object recognition using Histogram Of Gradient (HOG) and Support Vector Machine (SVM) methods. Finally, system is expected to recognize the appearance of the intruder and warn the house owner via some alarm notification. Prathibha et al. (2020) proposed a low cost Global System for Mobiles (GSM) based smart home security system that ensures face recognition. In this system, images of authorized per-

[41] http://jvde.us/info/x10_protocol.pdf.

sons are stored in the database. Then, when the detection occurs the camera captures the image from the live video streaming and compares it with the database. To save memory storage and power they use PIR sensors to activate the recording camera. Tanwar et al. (2017) also proposed an alert system for a smart home in order to detect an intruder or any unusual event that relies on PIR. Furthermore, the system provides a real-time email alert. Ji et al. (2018) designed a security protection system for smart home based on web technologies. It uses a type of micro-controller which uploads the indoor information collected by the sensor modules to the server through Wi-Fi module, and displays this information on the web page in real time. If there is any abnormal situation, it sends a message to the user's mobile terminal through the GSM module. Similarly, Nazir and Kaleem (2019) proposed a security system for a smart home based on the Message Queueing Telemetry Transport (MQTT) protocol to capture and transmit images for intrusion investigations. Butt et al. (2020) proposed a resident authentication approach for the home owner who relies on face recognition, voice recognition, and the Media Access Control (MAC) address of his/her smartphone. Yang et al. (2019) also proposed a very similar system. Jose and Malekian (2017) proposed a security approach that classifies the access points in a home as primary and secondary depending on their use. Then, with the help of a combination of sensors and micro-controllers, logic based sensing is implemented by identifying normal user behavior at these access points and requesting user verification when necessary. The user position is also considered when various access points changed states (the authors define some specific states adopted). Moreover, the algorithm also verifies the legitimacy of a fire alarm by measuring the change in temperature, humidity, and carbon monoxide levels, thus defending against manipulative attackers.

2) Network intrusion detection systems: Yuan et al. (2020) proposed an intrusion detection system for smart homes that relies on data augmentation and edge computing in order to address privacy problems related to data processing in the cloud computing environment. In this approach, network traffic is converted into images which are applied to train a Convolutional Neural Network (CNN) to classify the categories of network traffic. Furthermore, Auxiliary Classifier Generative Adversarial Network (AC-GAN) (Xia et al., 2018) is adopted to generate synthesized samples to expand the intrusion detection dataset. Ramapatruni et al. (2019) proposed an anomaly detection model for smart homes that relies on a Hidden Markov Model (HMM) that is trained on network level sensor data, created from a testbed with multiple sensors and smart devices in order to identify anomalous activities that can occur in a smart home environment. Serror et al. (2018) proposed an *in-network* approach that automatically adapts to the heterogeneity of smart home networks by restricting the communication capabilities of IoT devices without limiting their desired functionality. To this end, they proposed a rule-based network security mechanism that restricts both internal communication (i.e., with other devices in the same home network) and external communication (i.e., with Internet- and cloud-based services) of individual IoT devices to the extent necessary for supporting their intended functions. Pecorella et al. (2018) developed an approach that dynamically adapts the security level of the smart home network according to the user perceived risk level what they have called network sentiment analysis. The security level is not fixed. It is established by a central system, usually by the Internet Service Provider (ISP), but can be changed with the users cooperation. The security of the smart home network is improved by distributed firewalls and intrusion detection systems both at the smart home side and at the Internet service provider side. These two sides must cooperate and integrate their actions for reacting dynamically to new and ongoing threats. Moreover, the level of network sentiment detected can be propagated to nearby home networks (e.g., the smart home networks of the apartments inside a building) to increase/decrease their level of security, thus creating an intrusion protection system. In Cruz et al. (2015), proposed a security framework for home networks with residential gateways which are devices responsible for the exchange of information between the ISP infrastructure and the customer network to develop a large distributed Intrusion Detection System (IDS)/Intrusion Protection System (IPS), enforcing preventive or corrective countermeasures, according to the instructions issued by the ISP. Ghirardello et al. (2018) proposed a high level reference architecture which maps smart home products and services to facilitate security analysis on residential IoT systems. It comprises multiple viewpoints (functional viewpoint, physical viewpoint and communication viewpoint) through which a home automation network can be defined, each of which was chosen to describe the processes that enables IoT cloud platforms, the elements that comprise smart home devices and networks, and the methods through which device communications and interactions are possible. Nandi and Ernst (2016) proposed a technique that prevents errors due to too few triggers in the rules of firewalls. The technique statically analyzes a rules actions to determine what triggers are necessary. The approach eliminates a certain category of error (errors due to few triggers) in the rules. Then, the static analysis determines a necessary and sufficient set of trigger conditions for the rules. Barsocchi et al. (2018) proposed a security solution that relies on decoupling the different levels of control rules to maximize their effectiveness and to reduce as much as possible their maintenance and updates. The control levels considered are the Sensors Rules, which define the sensors behavior and activities; the Usage Control Rules, which define the users and sensors interactions; and the Access Control Rules, which manage the accesses to the different resources expressed through a specific control policy formalism. The purpose is to perform the continuous control and assessment of the smart home environment to improve the quality of life, safety and security of the people living, working, and visiting this environment.

3) Confidentiality/Authentication/Authorization systems: Shuai et al. (2019) proposed an anonymous authentication scheme for the smart home environment using Elliptic Curve Cryptography (ECC). The proposed scheme avoids keeping the verification table for authentication purposes and allows three types of mutual authentications: (1) between the user and the gateway node, (2) between the gateway node and the smart device, and (3) between the user and the smart device. Finally, a symmetric session key is established between the user and the smart device, which is used for future secure communications. In addition, the random number method (Hammi et al., 2017b) is adopted to prevent replay attacks, and it can avoid the clock synchronization problem (Wu et al., 2010). Sallam et al. (2019) proposed an approach that relies on Software Defined Perimeters to provide a more secure networking for the smart home all while ensuring lightweight authentication for devices as well as the dynamic update of firewall rules. Zeng and Roesner (2019) proposed a prototype smart home application that includes concrete features such as location-based access controls, supervisory access controls, and activity notifications. Demetriou et al. (2017) proposed *Hanguard*, a user-space mobile application that interfaces with the router to control access through Role-Based Access Control (RBAC). However this approach cannot stop attacks from a compromised companion application (Alrawi et al., 2019). Tao et al. (2018) proposed a multi-layer cloud architectural model in order to enable effective and seamless interactions/inter-operations on heterogeneous devices/services provided by different vendors in an IoT-based smart home. In addition, an ontology-based security service framework is designed for providing security and preserving privacy during the process of interactions/inter-operations on heterogeneous devices/services.

Table 2
Summary of existing smart home security solutions.

	Approach	Year	Techniques/ method/ technology used	Security goal									
				Human intrusion detection	Network Intrusion detection	Privacy	Confidentiality	Integrity	Authentication	Authorization	Non repudiation	Availability	Scalability
Surveillance/ alarm systems	Surantha and Wicaksono (2018)	2018	-Passive InfraRed (PIR) sensors -Histogram Of Gradient -Support Vector Machine	√	✗	✗	✗	✗	✗	✗	✗	✗	-
	Prathibha et al. (2020)	2020	-Global System for Mobiles (GSM) -PIR sensors	√	✗	✗	✗	✗	✗	✗	✗	✗	-
	Tanwar et al. (2017)	2017	-PIR sensors	√	✗	✗	✗	✗	✗	✗	✗	✗	-
	Ji et al. (2018)	2018	-Web server -GSM	√	✗	✗	✗	✗	✗	✗	✗	✗	✗
	Nazir and Kaleem (2019)	2019	-Message Queueing Telemetry Transport	√	✗	✗	✗	✗	✗	✗	✗	✗	-
	Butt et al. (2020)	2020	-Face recognition -Voice recognition	√	✗	✗	✗	✗	✗	✗	✗	✗	-
	Yang et al. (2019)	2019	- Image recognition -Speech recognition -Stereo matching algorithm	√	✗	✗	✗	✗	✗	✗	✗	✗	-
	Jose and Malekian (2017)	2017	-Logic based sensing	√	✗	✗	✗	✗	✗	✗	✗	✗	-
	Liang et al. (2021)	2021	-Zigbee based intruder detection system	√	✗	✗	✗	✗	✗	✗	✗	✗	✗

(*continued on next page*)

Table 2 (*continued*)

	Approach	Year	Techniques/ method/ technology used	Security goal									
				Human intrusion detection	Network Intrusion detection	Privacy	Confidentiality	Integrity	Authentication	Authorization	Non repudiation	Availability	Scalability
	Chiu et al. (2021)	2021	-Single-chip controlling unit -infrared sensors -IPCams motion detecting function	√	✗	✗	✗	✗	✗	✗	✗	✗	-
Network intrusion detection system	Yuan et al. (2020)	2020	-Data augmentation -Edge computing -Convolutional Neural Network -Auxiliary Classifier Generative Adversarial Network	✗	√	√	✗	✗	✗	✗	✗	✗	√
	Ramapatruni et al. (2019)	2019	-Hidden Markov Model	✗	√	✗	✗	✗	✗	✗	✗	✗	-
	Serror et al. (2018)	2018	-Rule-based network security	✗	√	√	✗	✗	✗	✗	✗	✗	-
	Pecorella et al. (2018)	2018	-Network sentiment analysis	✗	√	√	✗	✗	√	√	✗	✗	√
	Cruz et al. (2015)	2015	-Customer Premise Equipment Management Protocol -Rule-based network security	✗	√	√	✗	✗	√	√	✗	✗	✗

(*continued on next page*)

Table 2 (*continued*)

	Approach	Year	Techniques/ method/ technology used	Security goal									
				Human intrusion detection	Network Intrusion detection	Privacy	Confidentiality	Integrity	Authentication	Authorization	Non repudiation	Availability	Scalability
	Ghirardello et al. (2018)	2018	-Security architecture proposal	-	-	-	-	-	-	-	-	-	✗
	Nandi and Ernst (2016)	2016	-Automatic trigger generation	√	√	✗	✗	✗	✗	✗	✗	✗	-
	Barsocchi et al. (2018)	2018	-Rules access management -Middleware communication platform -Face recognition -K Nearest Neighbor algorithm	√	✗	√	✗	✗	√	√	✗	✗	-
	Bouwmeester et al. (2021)	2021	-Detection by the ISP -Contact the victims and provide a set of recommenda- tions	✗	√	-	√	√	√	-	-	√	✗
Confidentiality/ authentication/ Authorization systems	Shuai et al. (2019)	2019	-Elliptic Curve Cryptography	✗	√	√	√	√	√	√	√	✗	✗
	Sallam et al. (2019)	2019	-Software Defined Perimeters	✗	√	✗	✗	✗	✗	✗	✗	✗	✗
	Zeng and Roesner (2019)	2019	-Location-based access controls -Supervisory access controls -Activity notifications	√	✗	✗	✗	✗	√	√	✗	-	-

(*continued on next page*)

Table 2 (*continued*)

	Approach	Year	Techniques/ method/ technology used	Security goal									
				Human intrusion detection	Network Intrusion detection	Privacy	Confidentiality	Integrity	Authentication	Authorization	Non repudiation	Availability	Scalability
	Demetriou et al. (2017)	2017	-Software Defined Network -Role Based Access Control	✗	√	√	√	√	√	√	√	✗	✗
	Tao et al. (2018)	2018	-Ontology based security	✗	√	√	√	√	√	√	√	✗	√
	Chifor et al. (2018)	2018	-Cloud computing -Fast IDentity Online	✗	✗	√	✗	✗	√	√	✗	✗	√
	Alohali et al. (2014)	2014	-Cloud of Things -Symmetric key encryption	✗	√	√	√	✗	√	✗	✗	✗	✗
	Gunawan et al. (2019)	2019	-One Time PAD	✗	✗	✗	√	✗	✗	✗	✗	✗	✗
Blockchain based approaches	Lee et al. (2020)	2020	-Cloud computing -Private blockchain	✗	√	√	√	√	√	✗	√	√	√
	Fayad et al. (2018)	2018	-Preshared Key -Public blockchain	✗	√	√	√	√	√	√	√	√	√
	Hammi et al. (2018)	2018	-Secure virtual zones -Smart contracts -Public blockchain -Ethereum	✗	√	√	√	√	√	√	√	√	√
	Qashlan et al. (2020)	2020	-Private blockchain	✗	✗	✗	✗	√	√	✗	√	-	-

(*continued on next page*)

Table 2 (*continued*)

Approach	Year	Techniques/ method/ technology used	Security goal									
			Human intrusion detection	Network Intrusion detection	Privacy	Confidentiality	Integrity	Authentication	Authorization	Non repudiation	Availability	Scalability
Dorri et al. (2019)	2019	-Cloud computing -Private blockchain	✗	✗	✗	√	√	√	✗	√	✗	-
Zhou et al. (2018)	2018	-Private blockchain	✗	✗	✗	✗	√	√	✗	✗	✗	✗
Xu et al. (2018)	2018	-Private blockchain	✗	✗	✗	✗	√	✗	✗	✗	✗	✗
Aung and Tantidham (2017)	2017	-Private blockchain	✗	✗	✗	✗	√	✗	✗	✗	✗	✗
Singh et al. (2019)	2019	-Cloud computing -multivariate correlation analysis	✗	✗	-	√	√	✗	✗	✗	√	√
She et al. (2019); Stojkoska and Trivodaliev (2017)	2019	-Homomorphic consortium blockchain -Homomorphic encryption	✗	✗	√	√	√	√	✗	√	√	√
Arif et al. (2020)	2020	-Consortium blockchain	✗	✗	√	√	√	√	√	√	-	-
Ammi et al. (2021)	2021	-Private blockchain	✗	✗	√	√	√	√	√	√	√	-

Table 3
Classification of the recommendations proposed.

Manufacturer	End-user	Service providers	Legal society
Elliptic Curve Cryptography	Network segmentation	Advanced/lightweight authentication	Proposal of legislation for privacy/security
Physical protection	Advanced/lightweight authentication	Application stores filtering	Control of the legislation for privacy/security
Advanced/lightweight authentication	Changing factory settings	Network segmentation	

Chifor et al. (2018) proposed a lightweight authorization stack for smart home IoT applications. A smartphone component was implemented along with a password-less authentication protocol which is highly supported by many device manufacturers, using the Fast IDentity Online (FIDO) model (Ciolino et al., 2019). Finally, a theft resistant security scheme using a keep-alive protocol is executed periodically and every time the user requests a FIDO authentication through the cloud platform. A secure scheme for the Home Area Network (HAN) based on cloud computing has been proposed by Alohali et al. (2014). A Home Management System (HMS) manages devices and policies, and provides the access point for users. In the paper, the authors implemented the HMS functions in the cloud and the HMS interfaces with the cloud services. This scheme employs symmetric key encryption to ensure confidentiality for end-to-end communications and each smart object is assigned a unique key. Gunawan et al. (2019) applied the One Time Pad (OTP) encryption scheme to all the home communications to ensure their confidentiality. However, the OTP approach does not ensure the integrity and authentication security features, which allow numerous attacks (e.g., spoofing attack, and many others) to be executed.

4) Blockchain based approaches: Recently, numerous research efforts (Hammi et al., 2018; Hassija et al., 2019; Khan and Salah, 2018; Minoli and Occhiogrosso, 2018) have proposed the use of blockchains to ensure security in IoT. However, very few works have focused on their integration within a smart home use case. In this section we describe the main proposals in this area. These specific proposals can be grouped in the last categories that we considered (Surveillance/Alarm systems, Network intrusion detection systems and Confidentiality/Authentication/Authorization systems). However, we want to highlight their novel contributions which is why we discuss each of them separately.

In Lee et al. (2020), the authors proposed a blockchain-based smart home gateway network that mitigates possible attacks on the gateway of smart homes. Identification and data management for smart home gateways allow the ID and necessary information of the gateways to be recorded into the blocks in the blockchain. Devices connected to a smart home network register only those devices that are certified on the gateway. This information is added to blockchain blocks from time to time to identify the correct device and handle it through cryptographic communications, preventing data transmission from being leaked. The architecture classifies data entering the gateway so that the required data can be hashed, encrypted, and stored in the internal database. Fayad et al. (2018) proposed an adaptive blockchain based authentication and authorization approach for smart homes. In their proposed scheme, when a device needs to establish a communication session with the gateway, it sends it a Session Establishment Request (SEReq) that contains the objects ID and its authentication parameters (e.g., Pre-Shared Keys (PSK)). When the gateway receives the request, relying on the Object ID, it downloads from the blockchain the block containing the parameters related to that requested object. Then, the gateway decrypts the block and according to the retrieved parameters, it triggers the authentication operation. Next, a Session Establishment Response (SERep) is sent to the device to inform it whether it has been successfully authenticated or not. Finally, if the authentication is successful, then, the session establishment can be set up. Once the device is successfully authenticated and the session is established, the gateway controls each exchange and communication of the object relying on the list of authorization downloaded within the block.

In Hammi et al. (2018), the authors proposed a public blockchain based decentralized system that ensures robust identification and authentication of devices. The main goal of the proposed approach is to create secure virtual zones in IoT environments. Each device must communicate only with devices belonging to its zone, and considers every other device as malicious. These zones are called bubbles of trust. Thus, a smart home can be a bubble of trust where all its members can trust each other. It is protected and inaccessible to non-member devices which receive a certificate-like data structure for authentication purposes.

Qashlan et al. (2020) proposed a blockchain infrastructure to secure smart home transactions. Using private *Ethereum* blockchain, smart home IoT devices are configured. Smart contracts are built to specify the IoT devices behaviors on the network. Dorri et al. (2019) proposed a blockchain-based secure and lightweight architecture for a smart home. In their proposed scheme, the private blockchain in the smart home is centrally supervised by its owner. All communications between the local devices and the overlay nodes use a shared key issued by the miner to secure the communication. The author applied lightweight hashing to detect any deviation in the transactions. The proposed architecture assured data confidentiality, integrity, and availability. It also utilizes cloud storage to avoid the low memory issue for the smart home device. However, using a private blockchain can lead to numerous issues. Indeed, using a centralized node as miner/decider can lead to a single point of failure. Moreover, a proof of work/stake is the core activity that defends the blockchain against data forgery and double-spending attacks. However, this mechanism is absent in private blockchains. In Zhou et al. (2018), proposed a lightweight blockchain based smart home hierarchy architecture. In their proposed framework, every smart home has its own private blockchain and each IoT device stores a private distributed ledger. Devices can execute transactions by using smart contracts in the local chain. Due to storage limitations of smart home devices, each device uploads the chain to a local miner every 10 days and leaves only the last five blocks for the device. The local miner can design new smart contracts that allow the smart home devices to execute commands automatically based on user's preferences. However, this approach suffers from several drawbacks. First, limiting the chain to only five blocks goes against the principle of blockchain. Second, smart home devices are resource-constrained devices, thus a security approach must be lightweight and use minimum amount of computing and storage resources. Third, the scheme uses a private blockchain, which makes it suffer from the same drawbacks of Dorri et al. (2019). Xu et al. (2018) proposed an *Ethereum*-based decentralized smart home system. In their proposed design, smart contracts are utilized to store the data collected from the sensors in the blockchain to ensure the datas integrity. A similar approach was proposed by Aung and Tantidham (2017). However, both approaches suffer from private blockchain drawbacks as we have discussed above.

Singh et al. (2019) proposed an IoT smart home architecture based on cloud computing and blockchain technology to achieve

Table 4
Summary of some technical security risks related to smart homes, their impact and possible recommendations.[42]

Attribute	Risks and vulnerabilities	Security impact				Risk level				Recommendations
		Confidentiality	Integrity	Availability	Privacy	Critical	High	Medium	Low	
Software interfaces (e.g., smart TV interface, ...)	Default/weak password	√	✗	✗	√	-	-	√	-	Usage of long passwords that contains different characters types (numbers, lowercase letters, uppercase letters, special characters) - The password must be changed frequently
	Plugins downloaded from unknown sources	√	√	✗	√	-	√	-	-	Authorization of trusted sources only in order to prevent a built-in backdoors
	Outdated software/plugins	√	√	✗	√	-	-	√	-	All updates must be performed
	Default HTTP and HTTPS ports usage	✗	✗	√	√	-	-	-	√	Usage of non-default ports is preferable
	SSL/TLS deactivated	√	√	✗	√	-	√	-	-	At least another strong authentication/encryption protocol must be used
	No SSL certificate usage	√	√	✗	√	-	-	√	-	An authentication approach must be deployed
	Open remote access with root privileges	√	√	√	√	√	-	-	-	Root privileges must be limited to a set of controlled users
Network / gateways	Absence of strong security protocols (e.g., WPA2)	√	√	√	√	√	-	-	-	A strong authentication/encryption protocol must be used
	No hidden SSID name used	✗	✗	✗	√	-	-	-	√	
	Guest network absence	√	✗	✗	√	-	√	-	-	A separate network must be configured for house visitors and for ephemeral devices
	Absence of IP filtering absence	√	✗	✗	√	-	-	√	-	Only connections provided from trusted devices with known IP addresses must be accepted
	Absence of subnetworks partitioning	√	✗	✗	√	-	√	-	-	Network segmentation (e.g., using VLANs) must be performed in order to separate the devices of the different use case scenarios and to reduce the exposure of the devices traffic
Smart devices (e.g., speakers, locks, lights ...)	Outdated firmware	√	√	✗	√	-	-	√	-	All updates must be performed
	Absence of physical protection	√	√	√	√	-	√	-	-	Devices can be protected using hardware security modules which makes the critical information readable only by the device itself (FIP, 2001)
	Remote access not protected	√	√	√	√	√	-	-	-	Remote access must be authorized for a set of controlled users
	Non encryption of transmitted commands	√	√	√	√	√	-	-	-	Commands transmitted over the network, especially those of critical devices must be encrypted
	Non encryption of critical traffic	√	✗	✗	√	-	√	-	-	Lightweight encryption (e.g., ECC usage) must be used when possible
	Unsupervised physical access	√	✗	✗	√	-	√	-	-	Multi-factor authentication must be used when possible
	Overprivileged apps	√	√	✗	√	-	√	-	-	Thorough analysis is mandatory by apps providers

[42]HTTPS: HyperText Transfer Protocol Secure; SSL: Secure Sockets Layer; TLS: Transport Layer Security; WPA: Wi-Fi Protected Access; SSID: Service Set Identifier.

confidentiality, integrity, scalability, and availability to keep smart homes safe and secure. The blockchain is used to manage the devices transactions. The scheme also uses green cloud computing, which provides a green service using a green broker to reduce the environmental effects of the proposed model. Finally, it uses the multivariate correlation analysis technique to analyze the network traffic and identify the correlation among traffic features.

She et al. (2019); Stojkoska and Trivodaliev (2017) proposed a homomorphic consortium blockchain (a combination of public and private blockchain) for smart home system's sensitive data privacy preserving approach called HCB-SDPP. The scheme adds verification services via verification nodes to verify working nodes and transactions in the smart home environment. In order to record the home devices transactions, the authors proposed a new block data structure based on homomorphic encryption. They also proposed an encryption algorithm based on *Paillier* crypto-system for privacy protection. Finally, sensitive data of all gateway peers is encrypted and uploaded to the blockchain. Arif et al. (2020) also proposed a simple model to implement a secure architecture that utilizes a consortium blockchain. The home devices act as miners in the system. Indeed, some pre-selected nodes by the home owner in the system participate in the block creation and consensus. Moreover, a private mechanism has been provided for the users authorization and authentication to minimize the users involvement in the blockchain process. Finally, initial security checks are applied to the incoming request before getting into the blockchain process which ensures the confidentiality and integrity of data.

Discussion: Table 2 summarizes and compares the different security solutions discussed. We note that there are numerous approaches that have been proposed in the last few years aimed at protecting smart homes. Nevertheless, these works aim to achieve only one security goal such as intruder surveillance or ensuring authentication. Some of them such as (Chifor et al., 2018; Hammi et al., 2018; Jose and Malekian, 2017) ensure two or three main security goals/services. Thus, we can conclude that none of these previously proposed smart home architectures has considered the different security challenges and issues we have discussed in this paper. We also conclude that we need a comprehensive and holistic approach that ensures the security of smart homes and their occupants.

4.2. Recommendations

The *Open Web Application Security Project (OWASP)* and the *FBI* provide various recommendations to ensure smart homes security (Khan and Salah, 2018; Wells, 2020). They recommend to configure devices not to use default passwords and settings. Another recommendation is to use HyperText Transfer Protocol Secure (HTTPS) instead of HyperText Transfer Protocol (HTTP) along with firewalls. Moreover, firmware/software installed on devices should be updated regularly via encrypted communications. The file should be updated and downloaded from secure servers and the files must be signed and properly validated prior to installation. To regularly turn off microphone, cameras, and collection of personally information if possible. To refuse privileged requests that do not make sense.

Unfortunately, these recommendations are too general. But, most importantly, they cannot be applied in numerous scenarios. For example, (1) HTTPS cannot be used by all devices due to some devices constraints. (2) Generally consumers do not fully understand the applications privileges and so on which makes the security in smart homes a significant challenge. Thus, to ensure smart home security, we need both: (1) smart home devices manufacturers to implement the most suitable security solutions, and (2) users to be heavily involved by adopting best security practices. Relying on the different studies discussed above, we provide some recommendations and countermeasures. We stress that these are recommendations but to be fully effective in practice, there is a real need for new comprehensive proposals for smart home security.

Elliptic Curve Cryptography (ECC): ECC is known to be lightweight and can therefore be adapted to resource-constrained IoT devices (Hammi et al., 2020; Lauter, 2004). Even, if encryption is not possible, the IoT devices must at least use signature to enforce secure authentication as well as data integrity. For example, the *Elliptic Curve Digital Signature Algorithm (ECDSA)* has multiple benefits over traditional signature algorithms such as *Rivest Shamir Adleman (RSA)* especially in terms of key sizes and signature times (Hammi et al., 2018). Moreover, a timestamp verification can be added to counter replay attacks (the signature must cover the timestamp field).

Physical protection: There exist techniques that protect against node's physical compromise and the theft of secret/private keys, by making such information readable only by the device itself (FIP, 2001). Manufacturers of smart home devices must adopt such techniques.

Application stores filtering: App stores and providers must ensure a thorough analysis of the available apps by using appropriate techniques such as sandboxing in order to detect compromised apps or those with excessive privileges to access sensitive data.

Network segmentation: Network segmentation represents an efficient way to enhance the security of a home network. A required practical consideration is network segmentation between smart object, smart hubs, the Internet and the network used by consumers (Ferraris et al., 2019). If consumers segment their network, they will be able to implement IoT devices on one network and their normal devices on the other. Additionally, if an adversary gets access to the IoT network, it will reduce the risk of them getting access to other networks.

Legislation for privacy: To protect users privacy, new privacy policies must be imposed by governments and adopted by industry (Perez and Zeadally, 2017; Perez et al., 2018). In Europe, the General Data Protection Regulation (GDPR) shows promise in this direction in protecting user privacy. Other countries outside the European Union, could consider similar regulations. In the same context, the California Consumer Privacy Act (CCPA)[42] (Gilbert, 2020) that became effective in January 1st, 2020 represents a legislation that significantly expanded consumer privacy rights for California residents, imposing new business obligations on California businesses who have gross annual revenues in excess of $25 million, earn more than %50 of their revenue from selling consumers personal information, or buys, receives, or sells personal information of 50,000 or more households or consumers (Wells, 2020). Nonetheless, this law concerns only a set of companies and therefore it does not protect all the users.

Changing factory settings When a user installs a new device, he/she must change the default settings such as credentials. For a better security, legislation could also help. For example, the California Consumer Privacy Act (CCPA) enforces such obligations. Indeed, under CCPA, default passwords such as admin, 123456, and password are banned on all new electronic devices starting in 2020. The law specifically states that each new device will have a preprogrammed password specifically for that device, and that each device contain a security feature that requires the new owner to authenticate it prior to gaining access the first time (Gilbert, 2020).

Advanced/Lightweight authentication One-Time Password (OTP) is an authentication scheme in which a new password is generated for each authentication session and the reuse of a pass-

[42] https://www.sia-partners.com/en/trending-insights/california-consumer-privacy-act-ccpa.

Table 5
Acronym table.

Acronym	Meaning
AWS	Amazon Web Service
API	Application Programming Interface
AC-GAN	Auxiliary Classifier Generative Adversarial Network
BLE	Bluetooth Low Energy
BBC	British Broadcasting Corporation
CCPA	California Consumer Privacy Act
CIA	Central Intelligence Agency
CES	Consumer Electronics Show
CIRP	Consumer Intelligence Research Partners
C&C	Control and Command
CNN	Convolutional Neural Network
CRC	Cyclic Redundancy Check
DoS	Denial of Service
DDoS	Distributed Denial of Service
DDS	Distribution Service
DNS	Domain Name Service
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
FDI	False Data Injection
FIDO	Fast IDentity Online
FBI	Federal Bureau of Investigation
GDPR	General Data Protection Regulation
GSM	Global System for Mobiles
GHDB	Google Hacking Database
HVAC	Heating, Ventilation and Air-Conditioning
HMM	Hidden Markov Model
HOG	Histogram Of Gradient
HAN	Home Area Network
HMS	Home Management System
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
ICT	Information Communication Technology
IT	Information technology
IVA	Intelligent Virtual Assistants
IP	Internet Protocol
ISP	Internet Service Provider
IoT	Internet of Things
IDS	Intrusion Detection System
IPS	Intrusion Protection System
MAC	Media Access Control
MQTT	Message Queueing Telemetry Transport
NAS	Network Attached Storage
OTP	One Time Pad
OTP	One-Time Password
OWASP	Open Web Application Security Project
PIR	Passive InfraRed
PSK	Pre-Shared Keys
RCE	Remote Code Execution
RSA	Rivest Shamir Adleman
RBAC	Role-Based Access Control
SSH	Secure Shell
SSL	Secure Sockets Layer
SSID	Service Set IDentifier
SEReq	Session Establishment Request
SERep	Session Establishment Response
SPA	Smart Personal Assistant
SDN	Software Defined Networks
SQL	Structured Query Language
SVM	Support Vector Machine
TLS	Transport Layer Security
VLAN	Virtual Local Area Network
WPA2	Wi-Fi Protected Access 2

word is not possible (Hammi et al., 2020). OTP is one of the most promising solutions for authentication in IoT and smart homes environments. Therefore, its consideration (when it is possibly applicable) will limit replay attacks on symmetric-cryptography based devices.

Table 3 classifies the recommendations proposed. In the latter the risk level is estimated based on consequences of the possible attacks that can exploit the security flaw, on the infrastructure and their users (e.g., the absence of a strong authentication scheme can expose users data). Table 4 summarizes some of the most popular technical security risks and vulnerabilities in smart home ecosystems as well as their security impact and recommendations to mitigate them. Finally, Table 5 summarizes the different acronyms used in this paper.

5. Conclusion

The Internet had nine billion insecure IoT devices in 2017 (Wells, 2020). However, that number has increased drastically with the popularity of IoT in smart homes since then. According to Bhattiprolu (2020), it is expected to reach nearly 50 billion IoT devices by the year 2030. This means that the task of securing IoT devices in smart homes will become even more challenging than it already is.

As the costs of IoT devices continue to decline making them more affordable to home users, smart homes will continue to evolve and be adopted by many people. As a result, they will play an important role in the daily lives of people. Today, numerous home objects/appliances are being equipped with electronic devices and protocol suites in order to make them interconnected and connected to the Internet in order to provide security and comfort to home residents. The number of smart home devices, technologies and application scenarios keeps growing at a fast pace. This growth will increase the attack surface and expose users and residents to numerous security threats which have direct consequences on the residents and in some cases they can even cause harm or injury.

In this work we have presented an in-depth analysis of the security of the smart home ecosystem. We have investigated different cyberattacks and threats that can disrupt the proper functioning of diverse devices and services deployed in smart homes and we proposed a taxonomy for the latter. Then we discussed the various security and safety requirements and challenges that a smart home must face and we also proposed a taxonomy for it. Furthermore, we provided an extensive survey of recently proposed protection solutions for smart homes. Finally, we provided different recommendations that can help protect smart homes.

To the best of our knowledge, this work is the only holistic survey that focuses on the security of smart homes from different aspects (which include attacks, challenges, defense approaches, and recommendations) and reviews most of the existing surveys and reviews published in this area. For example, most of the recent publications on the topic of smart home security are fairly brief (typically 6 pages long) with many of them covering only a few security and threat aspects and cannot be considered to be extensive surveys. Moreover, numerous surveys are not dedicated to smart homes but consider them as an IoT use case and deals with them as such. Finally, it is well-known that many of the commercial products of the smart home market are the origin of most of the known security flaws. Therefore, it is necessary to consider the smart home system from an industry perspective and provide examples of real products, which we did in this survey but has not been addressed by most of the related surveys published to date on the topic of smart home security. For this reason, we did not only consider academic papers as sources, but we also reviewed many companies white papers, case studies, and surveys.

Following our analysis, we conclude that most of the smart home systems are vulnerable to a wide variety of cyberattacks. We also argue that none of the previously proposed smart security home architectures has considered the different security challenges and issues considered above. Therefore, we feel there is an urgent need for a comprehensive and holistic review that covers the security of smart homes and their occupants.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper

Acknowledgments

We thank the anonymous reviewers for their valuable comments which helped us improve the quality, content, and presentation of this paper. Sherali Zeadally was supported by a Fulbright U.S. scholar grant award administered by the U.S. Department of State Bureau of Educational and Cultural Affairs, and through its cooperating agency the Institute of International Education (IIE).

References

Ahmed, S.H., Zeebaree, S.R., 2021. A survey on security and privacy challenges in smarthome based IoT. Int. J. Contemp. Archit."The New ARCH" 8 (2), 489–510.
Albataineh, A., Alsmadi, I., 2019. IoT and the risk of internet exposure: risk assessment using Shodan queries. In: 2019 IEEE 20th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM). IEEE, pp. 1–5.
Ali, B., Awad, A.I., 2018. Cyber and physical security vulnerability assessment for IoT-based smart homes. Sensors 18 (3), 817.
Alohali, B., Merabti, M., Kifayat, K., 2014. A secure scheme for a smart house based on cloud of things (CoT). In: 2014 6th Computer Science and Electronic Engineering Conference (CEEC). IEEE, pp. 115–120.
Alrawi, O., Lever, C., Antonakakis, M., Monrose, F., 2019. Sok: Security evaluation of home-based IoT deployments. In: 2019 IEEE Symposium on Security and Privacy (SP). IEEE, pp. 1362–1380.
Ammi, M., Alarabi, S., Benkhelifa, E., 2021. Customized blockchain-based architecture for secure smart home for lightweight IoT. Inf. Process. Manage. 58 (3), 102482.
Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J.A., Invernizzi, L., Kallitsis, M., et al., 2017. Understanding the mirai botnet. In: 26th {USENIX} security symposium ({USENIX} Security 17), pp. 1093–1110.
Arif, S., Khan, M.A., Rehman, S.U., Kabir, M.A., Imran, M., 2020. Investigating smart home security: is blockchain the answer? IEEE Access 8, 117802–117816.
Atzori, L., Iera, A., Morabito, G., Nitti, M., 2012. The social internet of things (SIoT)–when social networks meet the internet of things: concept, architecture and network characterization. Comput. Netw. 56 (16), 3594–3608.
Aung, Y.N., Tantidham, T., 2017. Review of Ethereum: smart home case study. In: 2017 2nd International Conference on Information Technology (INCIT). IEEE, pp. 1–4.
Badis, H., Doyen, G., Khatoun, R., 2014. Toward a source detection of botclouds: a PCA-based approach. In: IFIP International Conference on Autonomous Infrastructure, Management and Security. Springer, pp. 105–117.
Barsocchi, P., Calabrò, A., Ferro, E., Gennaro, C., Marchetti, E., Vairo, C., 2018. Boosting a low-cost smart home environment with usage and access control rules. Sensors 18 (6), 1886.
Bastos, D., Shackleton, M., El-Moussa, F., 2018. Internet of things: a survey of technologies and security risks in smart home and city environments. In: IET Conference Proceedings. p. 30 (7 pp.)-30 (7 pp.)
Bhattiprolu, S., 2020. Securing IoT Applications for the Next Era of Industry: An Important Challenge and Opportunity. Technical Report. Nokia Software.
Biggio, B., Corona, I., Maiorca, D., Nelson, B., Šrndić, N., Laskov, P., Giacinto, G., Roli, F., 2013. Evasion attacks against machine learning at test time. In: Joint European Conference on Machine Learning and Knowledge Discovery in Databases. Springer, pp. 387–402.
Bitdefender, 2015. Remote Exploitation of the NeoCoolcam IP Cameras and Gateway. Technical Report. Bitdefender.
Bouwmeester, B., Rodríguez, E., Gañán, C., van Eeten, M., Parkin, S., 2021. "The thing doesn't have a name": learning from emergent real-world interventions in smart home security. In: Seventeenth Symposium on Usable Privacy and Security ({SOUPS} 2021), pp. 493–512.
Bugeja, J., Jacobsson, A., Davidsson, P., 2016. On privacy and security challenges in smart connected homes. In: 2016 European Intelligence and Security Informatics Conference (EISIC). IEEE, pp. 172–175.
Bugeja, J., Jönsson, D., Jacobsson, A., 2018. An investigation of vulnerabilities in smart connected cameras. In: 2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops). IEEE, pp. 537–542.
Butt, A.U.R., Qadir, M.A., Razzaq, N., Farooq, Z., Perveen, I., 2020. Efficient and robust security implementation in a smart home using the internet of things (IoT). In: 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE). IEEE, pp. 1–6.
Byun, J., Jeon, B., Noh, J., Kim, Y., Park, S., 2012. An intelligent self-adjusting sensor for smart home services based on ZigBee communications. IEEE Trans. Consum. Electron. 58 (3), 794–802.
Can, O., Sahingoz, O.K., 2015. A survey of intrusion detection systems in wireless sensor networks. In: 2015 6th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO). IEEE, pp. 1–6.
Cao, X., Shila, D.M., Cheng, Y., Yang, Z., Zhou, Y., Chen, J., 2016. Ghost-in-ZigBee: energy depletion attack on ZigBee-based wireless networks. IEEE Internet Things J. 3 (5), 816–829.
Chen, J., Liang, G., Cai, Z., Hu, C., Xu, Y., Luo, F., Zhao, J., 2016. Impact analysis of false data injection attacks on power system static security assessment. J. Mod. Power Syst. Clean Energy 4 (3), 496–505.
Chifor, B.-C., Bica, I., Patriciu, V.-V., Pop, F., 2018. A security authorization scheme for smart home internet of things devices. Future Gener. Comput. Syst. 86, 740–749.
Chitnis, S., Deshpande, N., Shaligram, A., et al., 2016. An investigative study for smart home security: issues, challenges and countermeasures. Wirel. Sens. Netw. 8 (04), 61.
Chiu, M.-C., Lai, W.-D., Chiu, C.-M., 2021. A smart home system with security and electrical appliances. J. Inf. Optim. Sci. 42 (2), 303–319.
Chung, H., Park, J., Lee, S., 2017. Digital forensic approaches for Amazon Alexa ecosystem. Digital Invest. 22, S15–S25.
Cimpanu, C., 2019. New silex malware is bricking IoT devices, has scary plans. Technical Report.
Ciolino, S., Parkin, S., Dunphy, P., 2019. Of two minds about two-factor: understanding everyday FIDO U2F usability through device comparison and experience sampling. Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019). USENIX Association.
da Costa, K.A., Papa, J.P., Lisboa, C.O., Munoz, R., de Albuquerque, V.H.C., 2019. Internet of things: a survey on machine learning-based intrusion detection approaches. Comput. Netw. 151, 147–157.
Cruz, T., Simões, P., Monteiro, E., Bastos, F., Laranjeira, A., 2015. Cooperative security management for broadband network environments. Secur. Commun. Netw. 8 (18), 3953–3977.
Das, A.K., Zeadally, S., He, D., 2018. Taxonomy and analysis of security protocols for internet of things. Future Gener. Comput. Syst. 89, 110–125.
Demetriou, S., Zhang, N., Lee, Y., Wang, X., Gunter, C.A., Zhou, X., Grace, M., 2017. HanGuard: SDN-driven protection of smart home WiFi devices from malicious mobile apps. In: Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks. Association for Computing Machinery, p. 122133.
Denning, T., Kohno, T., Levy, H.M., 2013. Computer security and the modern home. Commun. ACM 56 (1), 94–103.
Din, I.U., Guizani, M., Rodrigues, J.J., Hassan, S., Korotaev, V.V., 2019. Machine learning in the internet of things: designed techniques for smart cities. Future Gener. Comput. Syst. 100, 826–843.
Dorri, A., Kanhere, S.S., Jurdak, R., Gauravaram, P., 2019. LSB: a lightweight scalable blockchain for IoT security and anonymity. J. Parallel Distrib. Comput. 134, 180–197.
Edu, J.S., Such, J.M., Suarez-Tangil, G., 2020. Smart home personal assistants: a security and privacy review. ACM Comput. Surv. (CSUR) 53 (6), 1–36.
El-Hajj, M., Fadlallah, A., Chamoun, M., Serhrouchni, A., 2019. A survey of internet of things (IoT) authentication schemes. Sensors 19 (5), 1141.
FIPS PUB 140-2, 2001. Security requirements for cryptographic modules. Federal Information Processing Standards Publication.
Foreign Cyber Actors Target Home and Office Routers and Networked Devices Worldwide, 2018. Technical Report. Federal Bureau of Investigation (FBI).
Fayad, A., Hammi, B., Khatoun, R., 2018. An adaptive authentication and authorization scheme for IoT's gateways: a blockchain based approach. In: 2018 Third International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC). IEEE, pp. 1–7.
Fernandes, E., Jung, J., Prakash, A., 2016. Security analysis of emerging smart home applications. In: 2016 IEEE Symposium on Security and Privacy (SP). IEEE, pp. 636–654.
Fernández-Caramés, T.M., Fraga-Lamas, P., 2020. Teaching and learning IoT cybersecurity and vulnerability assessment with Shodan through practical use cases. Sensors 20 (11), 3048.
Ferraris, D., Fernandez-Gago, C., Daniel, J., Lopez, J., 2019. A segregated architecture for a trust-based network of internet of things. In: 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC). IEEE, pp. 1–6.
Gafurov, K., Chung, T.-M., 2019. Comprehensive survey on internet of things, architecture, security aspects, applications, related technologies, economic perspective, and future directions. J. Inf. Process. Syst. 15 (4), 797–819.
Genge, B., Enăchescu, C., 2016. ShoVAT: Shodan-based vulnerability assessment tool for internet-facing services. Secur. Commun. Netw. 9 (15), 2696–2714.
Ghirardello, K., Maple, C., Ng, D., Kearney, P., 2018. Cyber security of smart homes: development of a reference architecture for attack surface analysis. In: IET Conference Proceedings, vol. 45, p. 10.
Gilbert, A., 2020. California Consumer Privacy Act (CCPA) Compliance Guide: Everything You Need to Know About the New Data Privacy Law. Technical Report. ASANO.
Gopal, T.S., Meerolla, M., Jyostna, G., Eswari, P.R.L., Magesh, E., 2018. Mitigating mirai malware spreading in IoT environment. In: 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI). IEEE, pp. 2226–2230.
Gunawan, G., Lubis, A., Mubarakah, N., Jollyta, D., Effendi, S., et al., 2019. Smart home security design applying one time PAD algorithm. In: Journal of Physics: Conference Series, vol. 1361. IOP Publishing, p. 012040.

Hamad, S.A., Sheng, Q.Z., Zhang, W.E., Nepal, S., 2020. Realizing an internet of secure things: a survey on issues and enabling technologies. IEEE Commun. Surv. Tutor. 22 (2), 1372–1391.
Hammi, B., Doyen, G., Khatoun, R., 2014. Understanding botclouds from a system perspective: a principal component analysis. In: 2014 IEEE Network Operations and Management Symposium (NOMS). IEEE, pp. 1–9.
Hammi, B., Fayad, A., Khatoun, R., Zeadally, S., Begriche, Y., 2020. A lightweight EC-C-based authentication scheme for internet of things (IoT). IEEE Syst. J. 14 (3), 3440–3450.
Hammi, B., Khatoun, R., Zeadally, S., Fayad, A., Khoukhi, L., 2017. Iot technologies for smart cities. IET Netw. 7 (1), 1–13.
Hammi, B., Zeadally, S., Khatoun, R., 2019. An empirical investigation of botnet as a service for cyberattacks. Trans. Emerg. Telecommun.Technol. 30 (3), e3537.
Hammi, M.T., Hammi, B., Bellot, P., Serhrouchni, A., 2018. Bubbles of trust: a decentralized blockchain-based authentication system for IoT. Comput. Secur. 78, 126–142.
Hammi, M.T., Livolant, E., Bellot, P., Serhrouchni, A., Minet, P., 2017. A lightweight IoT security protocol. In: 2017 1st Cyber Security in Networking Conference (CSNet). IEEE, pp. 1–8.
Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., Sikdar, B., 2019. A survey on IoT security: application areas, security threats, and solution architectures. IEEE Access 7, 82721–82743.
He, D., Kumar, N., Zeadally, S., Vinel, A., Yang, L.T., 2017. Efficient and privacy-preserving data aggregation scheme for smart grid against internal adversaries. IEEE Trans. Smart Grid 8 (5), 2411–2419.
Herrmann, D.S., 2007. Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI. CRC Press.
Huang, L., Joseph, A.D., Nelson, B., Rubinstein, B.I., Tygar, J.D., 2011. Adversarial machine learning. In: Proceedings of the 4th ACM Workshop on Security and Artificial Intelligence, pp. 43–58.
Jason, H., Bill, D., Jody, G., Mary, W., Amy, T., Andrew, B., 2017. Cybersecurity in an IoT and Mobile World. Technical Report. ZDNet TechRepublic.
Ji, Y., Yang, Y., Huo, Z., 2018. Design of security protection system for smart home based on web. In: Proceedings of the 2nd International Conference on Computer Science and Application Engineering, pp. 1–6.
Jose, A.C., Malekian, R., 2017. Improving smart home security: integrating logical sensing into smart home. IEEE Sens. J. 17 (13), 4269–4286.
Kambourakis, G., Kolias, C., Stavrou, A., 2017. The mirai botnet and the IoT zombie armies. In: MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM). IEEE, pp. 267–272.
Kaspersky, 2020. Kaspersky Security Bulletin 2019. Statistics. Technical Report. Kaspersky.
Ken, H., Zhibin, Z., Ruchna, N., 2019. New Mirai Variant Targets Zyxel Network-Attached Storage Devices. Technical Report. Palo Alto.
Khan, M.A., Salah, K., 2018. IoT security: review, blockchain solutions, and open challenges. Future Gener. Comput. Syst. 82, 395–411.
Kolias, C., Kambourakis, G., Stavrou, A., Voas, J., 2017. Ddos in the IoT: mirai and other botnets. Computer 50 (7), 80–84.
Komninos, N., Philippou, E., Pitsillides, A., 2014. Survey in smart grid and smart home security: issues, challenges and countermeasures. IEEE Commun. Surv. Tutor. 16 (4), 1933–1954.
Konstantinou, C., Sazos, M., Musleh, A.S., Keliris, A., Al-Durra, A., Maniatakos, M., 2017. GPS spoofing effect on phase angle monitoring and control in a real-time digital simulator-based hardware-in-the-loop environment. IET Cyber-Phys. Syst. Theory Appl. 2 (4), 180–187.
Krejčí, R., Hujňák, O., Švepeš, M., 2017. Security survey of the IoT wireless protocols. In: 2017 25th Telecommunication Forum (TELFOR). IEEE, pp. 1–4.
Kubo, R., 2018. Detection and mitigation of false data injection attacks for secure interactive networked control systems. In: 2018 IEEE International Conference on Intelligence and Safety for Robotics (ISR). IEEE, pp. 7–12.
Kurakin, A., Goodfellow, I., Bengio, S., 2016. Adversarial machine learning at scale. arXiv preprint arXiv:1611.01236.
Labs, M., 2020. 2020 State of Malware Report. Technical Report. Malwarebytes Labs.
Labs, M., 2020. The Dark Side of Smart Lighting: Check Point Research Shows How Business and Home Networks Can Be Hacked from a Lightbulb. Technical Report. Check Point Software Technologies LTD.
Lauter, K., 2004. The advantages of elliptic curve cryptography for wireless security. IEEE Wirel. Commun. 11 (1), 62–67.
Lee, C., Zappaterra, L., Choi, K., Choi, H.-A., 2014. Securing smart home: technologies, security challenges, and security requirements. In: 2014 IEEE Conference on Communications and Network Security. IEEE, pp. 67–72.
Lee, Y., Rathore, S., Park, J.H., Park, J.H., 2020. A blockchain-based smart home gateway architecture for preventing data forgery. Hum.-Centric Comput. Inf. Sci. 10 (1), 1–14.
Liang, C.B., Tabassum, M., Kashem, S.B.A., Zama, Z., Suresh, P., Saravanakumar, U., 2021. Smart home security system based on Zigbee. In: Advances in Smart System Technologies. Springer, pp. 827–836.
Liang, G., Zhao, J., Luo, F., Weller, S.R., Dong, Z.Y., 2016. A review of false data injection attacks against modern power systems. IEEE Trans. Smart Grid 8 (4), 1630–1638.
Lin, H., Bergmann, N.W., 2016. IoT privacy and security challenges for smart home environments. Information 7 (3), 44.
Liu, X., Zhu, P., Zhang, Y., Chen, K., 2015. A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure. IEEE Trans. Smart Grid 6 (5), 2435–2443.
López, G., Quesada, L., Guerrero, L.A., 2017. Alexa vs. Siri vs. Cortana vs. Google assistant: a comparison of speech-based natural user interfaces. In: International Conference on Applied Human Factors and Ergonomics. Springer, pp. 241–250.
Marzano, A., Alexander, D., Fonseca, O., Fazzion, E., Hoepers, C., Steding-Jessen, K., Chaves, M.H., Cunha, Í., Guedes, D., Meira, W., 2018. The evolution of bashlite and mirai IoT botnets. In: 2018 IEEE Symposium on Computers and Communications (ISCC). IEEE, pp. 00813–00818.
Matherly, J., 2016. Complete guide to shodan. Shodan LLC 1, 1–70.
Minoli, D., Occhiogrosso, B., 2018. Blockchain mechanisms for IoT security. Internet of Things 1, 1–13.
Mocrii, D., Chen, Y., Musilek, P., 2018. IoT-based smart homes: a review of system architecture, software, communications, privacy and security. Internet of Things 1, 81–98.
Mohammad, Z.N., Farha, F., Abuassba, A.O., Yang, S., Zhou, F., 2021. Access control and authorization in smart homes: asurvey. Tsinghua Sci. Technol. 26 (6), 906–917.
Mohammadi, V., Rahmani, A.M., Darwesh, A.M., Sahafi, A., 2019. Trust-based recommendation systems in internet of things: a systematic literature review. Hum.-Centric Comput. Inf. Sci. 9 (1), 21.
Monteuuis, J.P., Hammi, B., Salles, E., Labiod, H., Blancher, R., Abalea, E., Lonc, B., 2017. Securing PKI requests for C-ITS systems. In: 2017 26th International Conference on Computer Communication and Networks (ICCCN). IEEE, pp. 1–8.
Musleh, A.S., Chen, G., Dong, Z.Y., 2019. A survey on the detection algorithms for false data injection attacks in smart grids. IEEE Trans. Smart Grid 11 (3), 2218–2234.
Nandi, C., Ernst, M.D., 2016. Automatic trigger generation for rule-based smart homes. In: Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security, pp. 97–102.
Nazir, S., Kaleem, M., 2019. Reliable image notifications for smart home security with MQTT. In: 2019 International Conference on Information Science and Communication Technology (ICISCT). IEEE, pp. 1–5.
Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G., Ghani, N., 2019. Demystifying IoT security: an exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations. IEEE Commun. Surv. Tutor. 21 (3), 2702–2733.
Nunziati, N., 2018. Did you Reboot Your Router Yet? Make Sure to do so and Soon. Technical Report. AVAST.
O'Donnell, L., 2019. Thousands of IoT Devices Bricked By Silex Malware. https://threatpost.com/thousands-of-iot-devices-bricked-by-silex-malware/146065/.
Osborne, C., 2014. Want to Send Spam? Hack the Fridge. Technical Report. ZDnet.
Osborne, C., 2018. IoT hacker builds Huawei-based botnet, enslaves 18,000 devices in one day. Technical Report. ZDnet.
Osborne, C., 2016. LizardStresser Botnet Targets IoT Devices to Launch 400Gbps Attacks. Technical Report. ZDnet.
Osborne, C., 2018. Mirai, Gafgyt IoT botnets stab systems with Apache Struts, SonicWall exploits. Technical Report. ZDnet.
Oregon FBI Tech Tuesday, 2019. Securing Smart TVs. Technical Report. Federal Bureau of Investigation (FBI). https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/tech-tuesdaysmart-tvs.
Palmer, D., 2020. This New Variant of Mirai Botnet Malware is Targeting Network-Attached Storage Devices. Technical Report. ZDnet.
Panwar, N., Sharma, S., Mehrotra, S., Krzywiecki, Ł., Venkatasubramanian, N., 2019. Smart home survey on security and privacy. arXiv preprint arXiv:1904.05476.
Papernot, N., McDaniel, P., Goodfellow, I., Jha, S., Celik, Z.B., Swami, A., 2017. Practical black-box attacks against machine learning. In: Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, pp. 506–519.
Park, D.-M., Kim, S.-K., Seo, Y.-S., 2019. S-mote: smart home framework for common household appliances in IoT network. J. Inf. Process. Syst. 15 (2), 449–456.
Park, J.-h., Salim, M.M., Jo, J.H., Sicato, J.C.S., Rathore, S., Park, J.H., 2019. CIoT-Net: a scalable cognitive IoT based smart city network architecture. Hum.-Centric Comput. Inf. Sci. 9 (1), 29.
Park, M., Oh, H., Lee, K., 2019. Security risk measurement for information leakage in IoT-based smart homes from a situational awareness perspective. Sensors 19 (9), 2148.
Pecorella, T., Pierucci, L., Nizzi, F., 2018. æNetwork sentimentg framework to improve security and privacy for smart home. Future Internet 10 (12), 125.
Perez, A.J., Zeadally, S., 2017. Privacy issues and solutions for consumer wearables. IT Prof 20 (4), 46–56.
Perez, A.J., Zeadally, S., Cochran, J., 2018. A review and an empirical analysis of privacy policy and notices for consumer internet of things. Secur. Privacy 1 (3), e15.
Prathibha, P., Kumar, A., Singh, A., Parul, K., Jaiswal, S., 2020. Smart home security system using IoT. Int. J. Res. Eng.Sci. Manage. 3 (5), 752–755.
Proofpoint, 2014. Your Fridge is Full of SPAM, Part II: Details. Technical Report. Proofpoint.
Proofpoint, 2014. Your Fridge is Full of SPAM: Proof of An IoT-driven Attack. Technical Report. Proofpoint.
Qashlan, A., Nanda, P., He, X., 2020. Automated Ethereum smart contract for block chain based smart home security. In: Smart Systems and IoT: Innovations in Computing. Springer, pp. 313–326.
Ramapatruni, S., Narayanan, S.N., Mittal, S., Joshi, A., Joshi, K., 2019. Anomaly detection models for smart home security. In: 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS). IEEE, pp. 19–24.

Rastogi, R., Jain, R., Jain, P., 2021. IoT applications in smart home security: addressing safety and security threats. In: Artificial Intelligence Paradigms for Smart Cyber-Physical Systems. IGI Global, pp. 251–277.
Rentz, P., 2019. Better Check This List: Worst Passwords of 2018. Technical Report. Techwell.
Rentz, P., 2019. OWASP Releases Latest Top 10 IoT Vulnerabilities. Technical Report. Techwell.
Ronen, E., Shamir, A., Weingarten, A.-O., OFlynn, C., 2017. IoT Goes Nuclear: Creating a Zigbee Chain Reaction. In: 2017 IEEE Symposium on Security and Privacy (SP). IEEE, pp. 195–212.
Sahinaslan, E., 2019. On the internet of things: security, threat and control. In: AIP Conference Proceedings, vol. 2086. AIP Publishing LLC, p. 030035.
Sallam, A., Refaey, A., Shami, A., 2019. Securing smart home networks with software-defined perimeter. In: 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC). IEEE, pp. 1989–1993.
Security, N., 2020. Shadow IoT: A Growing Threat to Enterprise Security. Technical Report. Net Security.
Seralathan, Y., Oh, T.T., Jadhav, S., Myers, J., Jeong, J.P., Kim, Y.H., Kim, J.N., 2018. IoT security vulnerability: a case study of a web camera. In: 2018 20th International Conference on Advanced Communication Technology (ICACT). IEEE, pp. 172–177.
Serror, M., Henze, M., Hack, S., Schuba, M., Wehrle, K., 2018. Towards in-network security for smart homes. In: Proceedings of the 13th International Conference on Availability, Reliability and Security, pp. 1–8.
She, W., Gu, Z.-H., Lyu, X.-K., Liu, Q., Tian, Z., Liu, W., 2019. Homomorphic consortium blockchain for smart home system sensitive data privacy preserving. IEEE Access 7, 62058–62070.
Shea, S., 2020. Smart Home or Building (Home Automation or Domotics). Technical Report. Techtarget.
Shokri, R., Stronati, M., Song, C., Shmatikov, V., 2017. Membership inference attacks against machine learning models. In: 2017 IEEE Symposium on Security and Privacy (SP). IEEE, pp. 3–18.
Shouran, Z., Ashari, A., Priyambodo, T., 2019. Internet of things (IoT) of smart home: privacy and security. Int. J. Comput. Appl. 182 (39), 3–8.
Shuai, M., Yu, N., Wang, H., Xiong, L., 2019. Anonymous authentication scheme for smart home environment with provable security. Comput. Secur. 86, 132–146.
Singh, S., Ra, I.-H., Meng, W., Kaur, M., Cho, G.H., 2019. SH-BlockCC: a secure and efficient internet of things smart home architecture based on cloud computing and blockchain technology. Int. J. Distrib. Sens. Netw. 15 (4). doi:10.1177/1550147719844159.
Singh Verma, R., Chandavarkar, B., 2019. Hard-coded credentials and web service in IoT: issues and challenges. Int. J. Comput. Intell. IoT 2 (3). Forthcoming
Stojkoska, B.L.R., Trivodaliev, K.V., 2017. A review of internet of things for smart home: challenges and solutions. J. Clean. Prod. 140, 1454–1464.
Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., Markakis, E.K., 2020. A survey on the internet of things (IoT) forensics: challenges, approaches and open issues. IEEE Commun. Surv. Tutor..
Surantha, N., Wicaksono, W.R., 2018. Design of smart home security system using object recognition and PIR sensor. Procedia Comput. Sci. 135, 465–472.
Tanwar, S., Patel, P., Patel, K., Tyagi, S., Kumar, N., Obaidat, M.S., 2017. An advanced internet of thing based security alert system for smart home. In: 2017 International Conference on Computer, Information and Telecommunication Systems (CITS). IEEE, pp. 25–29.
Tao, M., Zuo, J., Liu, Z., Castiglione, A., Palmieri, F., 2018. Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes. Future Gener. Comput. Syst. 78, 1040–1051.
Team, O.I.S., 2018. OWASP Top 10 Internet of Things 2018. Technical Report. The Open Web Application Security Project (OWASP).
Tiburski, R.T., Amaral, L.A., de Matos, E., de Azevedo, D.F., Hessel, F., 2017. Evaluating the use of TLS and DTLS protocols in IoT middleware systems applied to E-health. In: 2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC). IEEE, pp. 480–485.
Ünal, F., Almalaq, A., Ekici, S., Glauner, P., 2021. Big data-driven detection of false data injection attacks in smart meters. IEEE Access 9, 144313–144326.
U. 42, 2020. 2020 Unit 42 IoT threat report. Technical Report. Palo Alto Networks.
Urien, P., 2015. Innovative TLS/DTLS security modules for IoT applications: concepts and experiments. In: International Internet of Things Summit. Springer, pp. 3–15.
Verizon, 2020. Mobile Security Index 2020 Report: Mobile Security is the Key to Unlocking the Potential of Your Cloud, Internet and IoT. Technical Report. Verizon.
Viani, F., Robol, F., Polo, A., Rocca, P., Oliveri, G., Massa, A., 2013. Wireless architectures for heterogeneous sensing in smart home applications: concepts and real implementation. Proc. IEEE 101 (11), 2381–2396.
Vorobeychik, Y., Kantarcioglu, M., 2018. Adversarial machine learning. Synth. Lect. Artif. Intell.Mach. Learn. 12 (3), 1–169.
Worst Passwords of 2018, 2020. Techwell. Technical Report. Security TeamsID. https://www.techwell.com/techwell-insights/2019/01/better-check-list-worst-passwords-2018.
Wells, J., 2020. Better practices for IoT smart home security. Utica College.
Withanage, C., Ashok, R., Yuen, C., Otto, K., 2014. A comparison of the popular home automation technologies. In: Innovative Smart Grid Technologies-Asia (ISGT Asia), 2014 IEEE. IEEE, pp. 600–605.
Wu, Y., Wei, Z., Weng, J., Li, X., Deng, R.H., 2017. Resonance attacks on load frequency control of smart grids. IEEE Trans. Smart Grid 9 (5), 4490–4502.
Wu, Y.-C., Chaudhari, Q., Serpedin, E., 2010. Clock synchronization of wireless sensor networks. IEEE Signal Process. Mag. 28 (1), 124–138.
Xia, X., Togneri, R., Sohel, F., Huang, D., 2018. Auxiliary classifier generative adversarial network with soft labels in imbalanced acoustic event detection. IEEE Trans. Multimedia 21 (6), 1359–1371.
Xu, K., Wang, X., Wei, W., Song, H., Mao, B., 2016. Toward software defined smart home. IEEE Commun. Mag. 54 (5), 116–122.
Xu, Q., He, Z., Li, Z., Xiao, M., 2018. Building an Ethereum-based decentralized smart home system. In: 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS). IEEE, pp. 1004–1009.
Xu, W., Qi, Y., Evans, D., 2016. Automatically evading classifiers. In: Proceedings of the 2016 Network and Distributed Systems Symposium, vol. 10.
Yang, A., Zhang, C., Chen, Y., Zhuansun, Y., Liu, H., 2019. Security and privacy of smart home systems based on the internet of things and stereo matching algorithms. IEEE Internet Things J. 7 (4), 2521–2530.
Yuan, D., Ota, K., Dong, M., Zhu, X., Wu, T., Zhang, L., Ma, J., 2020. Intrusion detection for smart home security based on data augmentation with edge computing. In: ICC 2020 IEEE International Conference on Communications (ICC). IEEE, pp. 1–6.
Zeadally, S., Adi, E., Baig, Z., Khan, I.A., 2020. Harnessing artificial intelligence capabilities to improve cybersecurity. IEEE Access 8, 23817–23837.
Zeadally, S., Das, A.K., Sklavos, N., 2021. Cryptographic technologies and protocol standards for internet of things. Internet of Things 14, 100075.
Zeadally, S., Pathan, A.-S.K., Alcaraz, C., Badra, M., 2013. Towards privacy protection in smart grid. Wirel. Pers. Commun. 73 (1), 23–50.
Zeng, E., Roesner, F., 2019. Understanding and improving security and privacy in multi-user smart homes: a design exploration and in-home user study. In: 28th {USENIX} Security Symposium ({USENIX} Security 19), pp. 159–176.
Zhou, Y., Han, M., Liu, L., Wang, Y., Liang, Y., Tian, L., 2018. Improving IoT services in smart-home using blockchain smart contract. In: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, pp. 81–87.
Zou, X., 2019. IoT Devices are Hard to Patch: Here's Why–and How to Deal with Security. Technical Report. Techbeacon.

Badis Hammi is an associate professor in EPITA Engineering School, France. He received a doctoral degree in computer science from Troyes University of Technology in 2015. Then, he held a research position at Institut Mines Telecom ParisTech, France. His research interests include cybersecurity and privacy in computer networks and systems.

Sherali Zeadally is an associate professor in the College of Communication and Information at the University of Kentucky. He received his Bachelors degree in computer science from the University of Cambridge, England, and his doctoral degree in computer science from the University of Buckingham, England. He is a Fellow of the British Computer Society and a Fellow of the Institution of Engineering Technology, England.

Rida Khatoun received his MSc in Computer Engineering and the PhD from the University of Technology of Troyes (UTT) in France in 2004 and 2008. He is currently Associate Professor at Telecom ParisTech. His current areas of research interest include Cloud Computing Security, Internet of Things Security, Vehicular Networks Security, Security Architecture, Intrusion Detection System and Blockchain technology.

Jamel Nebhen received the MSc degree in microelectronics from the National School of Engineering of Sfax, Tunisia, in 2007, and the PhD degree in microelectronics from Aix-Marseille University, France, in 2012. From 2012 to 2018, he worked as a Postdoctoral Researcher with LIRMM-Lab Montpellier, France, IM2NP-Lab Marseille, ISEP Paris, LE2I-Lab Dijon, Lab-Sticc Telecom Bretagne Brest, and IEMN-Lab Lille. Since 2019, he has been as an Assistant Professor with Prince Sattam Bin Abdulaziz University, Alkharj, Saudi Arabia. His research interests include design of analog and RF integrated circuits, the IoT, biomedical circuit, and sensors instrumentation.