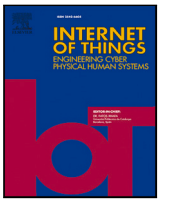
Internet of Things 20 (2022) 100588

Contents lists available at ScienceDirect

Internet of Things

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



Review article

A survey on blockchain, SDN and NFV for the smart-home security

N'guessan Yves-Roland Douha [a,*], Monowar Bhuyan [b], Shigeru Kashihara [c], Doudou Fall [d], Yuzo Taenaka [a], Youki Kadobayashi [a]

[a] Graduate School of Science and Technology, Nara Institute of Science and Technology, 630-0192, Ikoma, Japan
[b] Department of Computing Science, Umeå University, SE 901 87, Umeå, Sweden
[c] Faculty of Information Science and Technology, Osaka Institute of Technology, Osaka, 573-0196, Japan
[d] Ecole Supérieure Polytechnique, University Cheikh Anta Diop, Dakar, Senegal

ARTICLE INFO

Keywords:
Smart homes
IoT
Privacy
Security
Trust
Blockchain
SDN
NFV

ABSTRACT

Due to millions of loosely coupled devices, the smart-home security is gaining the attention of industry professionals, attackers, and academic researchers. The smart home is a typical home where many sensors, actuators, and IoT devices are used to automate home users' daily activities. Although a smart home provides comfort, safety, and satisfaction to users, it opens up multiple challenging security issues when automating and offering intelligent services. Recent studies have investigated not only blockchain but SDN and NFV to address these challenges. We present a comprehensive survey on blockchain, SDN, and NFV for smart-home security. The paper also proposes a new architecture of the smart-home security. First, we describe the features of the smart home and its current security issues. Next, we outline the characteristics of blockchain, SDN, and NFV, including their contribution to improving the smart-home security. While SDN enhances the management and access control of the home network by providing a programmable controller to home nodes, NFV implements the functions of network appliances (e.g., network monitoring, firewall) as virtual machines and ensures the high availability of the network. Blockchain reinforces IoT data's privacy, integrity, and security and improves the trust in transactions among untrusted IoT devices. Finally, we discuss open issues and challenges in the field and propose recommendations towards high-level security for the smart home.

1. Introduction

The Internet of Things (IoT) is a disruptive technology that brings human beings and the cyberspace closer. Traditional daily life items (e.g., refrigerators, watches, and light bulbs) are nowadays turned "smart" by embedding sensors and actuators. IoT devices are useful since they support users' daily life. For instance, smartwatches can monitor heart rate and significantly contribute in various ways to the health and wellness of users [1]. A smart home is an IoT application that promotes technology-based living places. Jiang et al. [2] defined this home as "a dwelling incorporating a communications network that connects the key electrical appliances and services, and allows them to be remotely controlled, monitored or accessed". Statista estimates that the worldwide revenue of smart homes, US$78.9 billion in 2020, will increase to US$182.3 billion by 2025 [3]. This IoT-based home attracts considerably, not only normal users, but also attackers.

* Corresponding author.
E-mail addresses: douha.nguessan_yves-roland.dn6@is.naist.jp (N.Y.-R. Douha), monowar@cs.umu.se (M. Bhuyan), shigeru.kashihara@oit.ac.jp (S. Kashihara), doudou.fall@esp.sn (D. Fall), yuzo@is.naist.jp (Y. Taenaka), youki-k@is.naist.jp (Y. Kadobayashi).

https://doi.org/10.1016/j.iot.2022.100588
Received 15 April 2022; Received in revised form 15 July 2022; Accepted 3 August 2022
Available online 23 August 2022

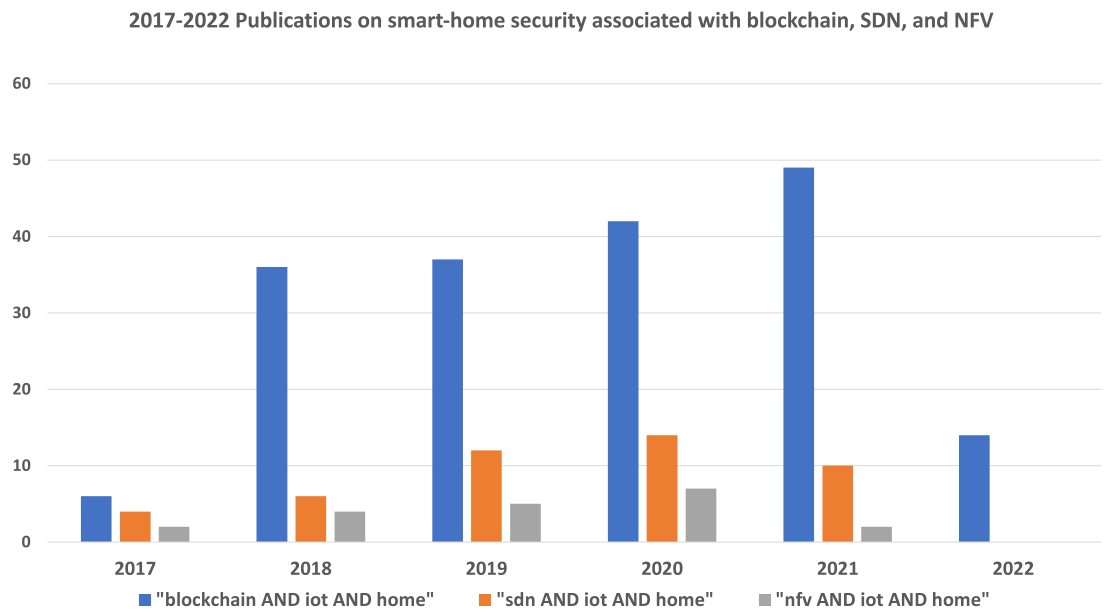


Fig. 1. An overview of evolutionary trends from 2017 to 2022 in the number of published papers covering blockchain, SDN, NFV, and smart-home security. The report reflects source items indexed in "Web of Science Core Collection".

In 2021, 60.1 million IoT attacks were recorded, resulting in a 6% year-over-year increase [4]. The proliferation of IoT attacks targeting smart-home devices could impact the quality of life of smart-home users. Hence, it is urgent and important to focus on the smart-home security.

The heterogeneity and complexity of the smart-home environment cause the need for more efficient technologies to ensure access control management and data privacy, integrity, and security in smart homes. Recent technologies, more particularly blockchain [5], SDN [6], and NFV [7] have been explored to address smart-home security issues by strengthening confidentiality, integrity, availability, flexibility, interoperability, and mitigating cyberattacks. The use of blockchain builds trust in the IoT network composed of untrusted IoT devices. SDN improves the management and access control of the smart-home network. NFV focuses on the high availability of the smart-home network to allow users to access their services on demand. Each of these contributions could solve some of the security issues in smart homes. In the recent past years, Web of Science [8], a world-leading citation database, has registered numerous published papers associated with the topics *"blockchain AND iot AND home"*, *"sdn AND iot AND home"*, and *"nfv AND iot AND home"*. These papers relate to crucial information security principles such as confidentiality, integrity, availability, privacy, and trust—which are among the factors that contribute to keeping users and their data safe and secure. Fig. 1 shows the recent growing interests of researchers in these three technologies for securing smart homes. Moreover, previous research papers have demonstrated that using "SDN and NFV [9]", "blockchain and SDN [10]", and "blockchain, SDN, and NFV [11]" could improve the security architecture of IoT systems. Therefore, there is a need to investigate the security values that blockchain, SDN, and NFV could provide towards a more secure and resilient smart home and design a new multilevel security architecture using these technologies for the smart-home security.

1.1. Contributions

This survey analyzes the recent studies on the smart-home security. In addition, the survey provides a structured and comprehensive overview of vulnerabilities and attacks on smart homes, technologies (i.e., blockchain, SDN, and NFV) aware security solutions for smart homes. Furthermore, the survey presents the security performance evaluation of smart homes. Finally, the survey discusses the open issues, challenges, and recommendations related to the blockchain, SDN, and NFV for the smart-home security.

The following are the major contributions.

- We discuss smart-home technologies and security issues. We describe the core components and functions that make smart homes convenient and attractive. Furthermore, we present the existing security issues such as vulnerabilities of smart homes and cyberattacks targeting smart homes.
- We highlight and analyze the advantages of using blockchain, SDN, and NFV for the smart-home security. We meticulously explain how each technology works and describe essential concepts and processes. These descriptions help readers have a quick and thorough understanding of the potential of these technologies.

Table 1
List of essential acronyms and abbreviations.

Label	Description	Label	Description	Label	Description
3G	Third (3rd) Generation of mobile technologies and services	IP	Internet Protocol	OWASP	Open Web Application Security Project
A11y	Accessibility	IPS	Intrusion Prevention System	PoP	Point of Presence
ACC	Access Control Contract	ISO	International Organization for Standardization	PoS	Proof of Stake
ACL	Access Control List	ISO-KE	ISO Key Encryption protocol	PoW	Proof of Work
AI	Artificial Intelligence	ISP	Internet Service Provider	PBFT	Practical Byzantine Fault Tolerance
AMQP	Advanced Message Queuing Protocol	IT	Information Technology	RAM	Random Access Memory
ANASTACIA	Advanced Networked Agents for Security and Trust Assessment in CPS/IoT Architectures	JC	Judge Contract	RC	Register Contract
API	Application Programming Interface	KNN	K-Nearest Neighbor	RF	Random Forest
ARP	Address Resolution Protocol	LAN	Local Area Network	ROC	Receiver Operating Characteristic
ASR	Automated Speech Recognition	LK-SVM	Linear Kernel SVM	ROP	Return-Oriented Programming
BLE	Bluetooth Low Energy	LoRaWAN	Long Range Wide Area Network	RPL	Routing Protocol for Low-Power
CD	Compact Disc	LTE-M	Long Term Evolution category M1	SDHN	Software-defined Home Networks
CIA	Confidentiality Integrity Availability	MANO	Management and Orchestration	SDN	Software-Defined Networking
CVE	Common Vulnerabilities and Exposures	MITM	Man-In-The-Middle	SHAS	Smart-Home Automation Systems
DDoS	Distributed Denial of Service	ML	Machine Learning	SIGMA	SIGn-and-MAc
DoS	Denial of Service	MRIP	Multiple Replications In Parallel	SQL	Structured Query Language
DTLS	Datagram Transport Layer Security	MUD	Manufacturer Usage Description	SVM	Support Vector Machine
ECDSA	Elliptic Curve Digital Signature Algorithm	NETCONF	Network Configuration	TLS	Transport Layer Security
FATS	Fingerprint and Timing-based Snooping	NETRA	NFV-based Edge Traffic Analysis	TV	Television
FPGA	Field Programmable Gate Arrays	NFV	Network Functions Virtualization	VCS	Voice Controllable Systems
GNS3	Graphic Network Simulator 3	NFVI	NFV Infrastructure	VIM	Virtualized Infrastructure Manager
GVS	Google Voice Search	NFVO	NFV Orchestrator	VLAN	Virtual LAN
HLS	High-level synthesis	OFX	OpenFlow Extension Framework	VM	Virtual Machine
HVAC	Heating, Ventilation, and Air Conditioning	OMNeT++	Objective Modular Network Testbed in C++	VNF	Virtualized Network Function
ID	Identity	ONOS	Open Network Operating System	VNFM	VNF Manager
IDC	International Data Corporation	OPNET	Optimum Network Performance	VPA	Virtual Personal Assistant
IDS	Intrusion Detection System	OPNFV	Open Platform for NFV	WAP	Wireless Access Point
IEMI	Intentional Electromagnetic Interference	OSI	Open System Interconnection	Wi-Fi	Wireless Fidelity
IoT	Internet of Things	OVS	Open vSwitch	WPAN	Wireless Personal Area Network

- We discuss simulation tools, datasets, and metrics for the analysis of smart-home networks. Measuring network security performances is also essential to maintain service availability in a smart home and validate any proposed method aiming to improve the smart-home security. However, the existing literature does not provide interested readers with comprehensive details regarding these instruments.
- We present several open issues and challenges in design, implementation, and deployment viewpoints. The development and vulgarization of smart-home technologies and their security are not mature yet. We discuss challenges that need to be solved to improve the adoption of smart homes and ensure users' safety and security.
- Finally, we present our recommendations to academic researchers, industry professionals, and all those who are interested in designing, developing solutions for the smart-home security. Furthermore, we propose a new smart-home architecture that takes advantage of blockchain, SDN, and NFV to cope with major security issues of smart homes.

1.2. Organization

Table 1 describes the essential acronyms and abbreviations in this survey. The rest of the paper is organized as follows. Section 2 analyzes the related work and compares them with our survey. Section 3 describes the smart-home technology. In Section 4, we present the security issues in smart homes. Section 5 outlines technologies aware security solutions explored in this paper. Sections 6, 7, and 8 respectively describe the contributions of blockchain, SDN, and NFV in the enhancement of the smart-home security. Section 9 presents an architecture of smart homes based on these technologies. Section 10 presents tools, datasets, and metrics for performance evaluation of the smart-home security. Section 11 discusses the open issues and challenges in smart-home security and presents our recommendations to mitigate these issues. Section 12 concludes this study.

2. Related work

This section presents recent survey papers on the smart-home security from 2018 to date and shows the contribution of our paper compared to the existing literature.

Bastos et al. [12] present a survey of IoT technologies and security issues in smart home and city environments. The focus of this survey is on securing communications in IoT. The authors suggest a new approach to data protocols using intrinsic security capabilities, defense-in-depth strategies, and lightweight encryption and decryption. They mention several security aspects such as privacy, confidentiality, integrity, availability, and authentication. However, this work does not highlight the importance of access control and trust which are also essential to ensure the security of IoT networks. Khawla et al. [13] describe smart-home applications and classify the communication protocols (e.g., LoRaWAN, RPL, DTLS, AMQP) regarding the OSI model. They also discuss smart-home security issues and recommend the implementation of good practices such as security by design and the raising of consumers' awareness to improve the smart-home security environments. In contrast with Bastos et al. [12], this highlights the importance of access control in smart homes. However, the authors do not highlight the importance of availability and trust. Mocrii et al. [14] emphasize the importance of trust using blockchain for the smart-home security. In addition, the authors describe the significant technologies (e.g., cloud, software, network) in smart homes. According to the authors, privacy and security should be the top priority in smart-home technologies. In addition, they mention two types of threats: the internal (short-distance) attacks and the external (Internet-based) attacks. To cope with these threats, the authors propose a general awareness of all stakeholders of the smart home ecosystem, including the vendors, service providers, and consumers. Furthermore, they recommend the blockchain technology, as a trusted platform, to guarantee the safety and security of data storage and computing infrastructure of smart homes. However, this survey paper does not mention many security aspects (e.g., confidentiality, integrity, availability, authentication, and access control). Barriga and Yoo [15] also show the importance of blockchain for the smart-home security. They describe approaches to ensure privacy, security, authentication in smart homes using blockchain for securing event logging systems and SDN for securing the smart-home gateways from cyberattacks. However, this work does not discuss availability as a requirement for smart home security.

Moreover, Kuyucu et al. [16] present several security issues in the smart-home environment. The authors discuss security, privacy, and authentication issues and review the current literature proposing specific solutions to address the existing vulnerabilities in smart homes. However, this work does not highlight security requirements such as access control, trust, and the CIA triad (i.e., confidentiality, integrity, availability). As for Panwar et al. [17], the authors discuss the CIA triad. However, privacy, authentication, access control, and trust are not part of the work. The authors study the security protocols involved in device-to-device communication and those used between users' terminals and the cloud. As a result, they propose lightweight cryptographic solutions (i.e., International Organization for Standardization key encryption protocol (ISO-KE), Okamoto identification scheme, Pedersen commitment scheme, Schnorr identification scheme, SIGn-and-MAc (SIGMA), and Transport Layer Security (TLS)) as security protocols in smart homes.

Sarhan [18] provides an overview of the state-of-the-art contributions in smart-home safety and security systems using Arduino. In addition, the author analyzes, classifies, compares, and discusses the applications, the enabling sensors, the Arduino boards, the alert notifications, the data storage servers, and the architectures of the reviewed papers from different perspectives. Furthermore, the author presents many challenges related to the use of Arduino in smart-home safety and security. The work does not consider security requirements such as privacy, confidentiality, integrity, access control, and trust. AlJanah et al. [19] cover most security requirements. The authors present a systematic analysis of security issues and threats related to authentication in a smart-home environment. They critically analyze existing authentication solutions for IoT environments and specify a list of security requirements for a robust authentication system in a smart home. However, they do not discuss privacy, access control, and trust.

Based on previous work, using blockchain and SDN could help improve the smart-home security. In [20], Khan and Salah describe and map security issues regarding the IoT layered architecture, which includes three layers: physical, transport, and application layers. The authors use blockchain to solve open security issues in IoT relating to authentication and data privacy, identity and access management of IoT devices, trustworthy decentralized management, governance, and lightweight security protocols to secure the communication of IoT devices. In [21], the authors describe security issues in IoT security and countermeasures. This work presents the advantages of SDN and NFV for the reinforcement of IoT security. However, the authors do not focus on the smart-home security, whose security challenges are different from other IoT applications due to the home context and human factor.

Only a few works discuss the advantages of blockchain, SDN, and NFV in IoT and smart-home security. For these reasons, we have decided to propose a novel comprehensive survey of the smart-home security based on these technologies. Table 2 presents the security concerns discussed in the existing works mentioned above. Each paper provides state-of-the-art literature on the smart-home security. However, as we can see in this table, recent survey papers do not fully cover important security aspects such as privacy, security, confidentiality, integrity, availability, authentication, access control, and trust. In addition, only a few survey papers highlight the benefits of blockchain and SDN for the smart-home security. Our survey fully covers multiple security aspects, emphasizes the contribution of blockchain, SDN, and NFV, and provides the most recent state-of-the-art of this topic with significant contributions. Furthermore, in contrast to the related work, this paper sheds light on smart-homes core components, attack types targeting smart homes, public datasets for intrusion detection in smart homes, and simulation tools and metrics for analyzing smart-home networks.

Table 2
Comparison with the state-of-the-art surveys of the smart-home security.

Features	Surveys								
	Bastos et al. [12] (2018)	Khawla et al. [13] (2018)	Mocrii et al. [14] (2018)	Barriga and Yoo [15] (2018)	Kuyucu et al. [16] (2019)	Panwar et al. [17] (2019)	Sarhan et al. [18] (2020)	AlJanah et al. [19] (2021)	Our paper (2022)
Privacy	✓	✓	✓	✓	✓	X	X	X	✓
Security	✓	✓	✓	✓	✓	✓	✓	✓	✓
Confidentiality	✓	✓	X	✓	X	✓	X	✓	✓
Integrity	✓	✓	X	✓	X	✓	X	✓	✓
Availability	✓	X	X	X	X	✓	✓	✓	✓
Authentication	✓	✓	X	✓	✓	X	X	✓	✓
Access control	X	✓	X	✓	X	X	X	✓	✓
Trust	X	X	✓	✓	X	X	X	X	✓
Blockchain	X	X	✓	✓	X	X	X	X	✓
SDN	X	X	X	✓	X	X	X	X	✓
NFV	X	X	X	X	X	X	X	X	✓

3. Smart-home technology

A smart home is a house that uses IoT devices adapted to households' needs. It differs from other applications of IoT technology because of the typical features it offers users. For example, the IoT in agriculture (i.e., smart agriculture) uses sensors to collect data, such as weather conditions and soil quality, to monitor crop growth and detect anomalies that could lead to crop damage. As for smart homes, the sensors and IoT devices could detect human inactivity and reduce the energy consumption of non-critical smart-homes devices, such as smart light bulbs. The smart home includes various components, functions, and technologies. In Fig. 2, we present an overview of a smart home. This figure illustrates the significant functions of the smart home as well as some IoT devices, network technologies, and cloud computing. In the proposed illustration, the automation function describes the interconnection of IoT devices through wireless communications, e.g., Zigbee, Wi-Fi. IoT devices are classified regarding their primary goals, e.g., smart cameras for safety and security.

3.1. Core components

We categorize the major components of smart homes into four elements, including devices, networks, applications, and cloud infrastructures. The smart-home devices include user's terminals (e.g., smartphones, tablets, and computers), network devices (e.g., gateway, firewall, switch, and router), and IoT devices. IoT devices cover many areas, such as energy (e.g., smart meter and smart light bulb), healthcare (e.g., smart contact lens, smartwatch, and smart bed), safety and security (e.g., smart fire alarm, smart camera, and smart door lock), and entertainment (e.g., smart speaker and smart television (TV)). The smart-home network comprises Ethernet and Wireless technologies (e.g., ZigBee, Z-Wave, BLE, Wi-Fi, SigFox, and LTE-M). The smart-home applications are mainly mobile and web applications that manage the smart-home devices through user's terminals. The cloud infrastructures process IoT data and allows home users to control their home appliances remotely over the Internet.

3.2. Core functions

Smart homes achieve various goals such as management of energy consumption, safety, security, healthcare, and entertainment [22]. Smart homes enable energy management. Living in a smart home helps to save energy consumption and money [23]. Users can set up devices to make them turn on or turn off automatically. In addition, smart homes also provide safety and security. When users are far away from their homes, they could use smart cameras to talk remotely to unfamiliar visitors, and these cameras could monitor in the dark as well. Furthermore, in case of emergency (e.g., fire alarm, anti-theft alarm), smart homes could notify users, their families, or the police. Healthcare is another core function of smart homes. The elderly could leverage healthcare services to get assistance 24/7. In 2017, the United Nations reported that the number of older persons is projected to increase and reach nearly 2.1 billion by 2050, and the elderly will live more and more independently [24]. Smart homes could provide them assistance in their daily life (e.g., medical monitoring) [25]. Furthermore, smart homes help to relax and have fun as well. When getting tired, users could enjoy their favorite TV shows, songs, movies, online games by watching the smart TV. For instance, from one voice command, users could transform their smart homes into movie theaters and have a good time. Finally, we include home automation as a core function of smart homes. IoT devices interact with each other and automate users' activities. While the number of well-defined tasks could limit IoT devices, robots have more autonomy and can handle unexpected situations [26]. Robots can also support the daily activities of users. For instance, Wilson et al. [27] emphasize the contribution of physical robots to aid in completing daily activities of users, such as senior citizens.

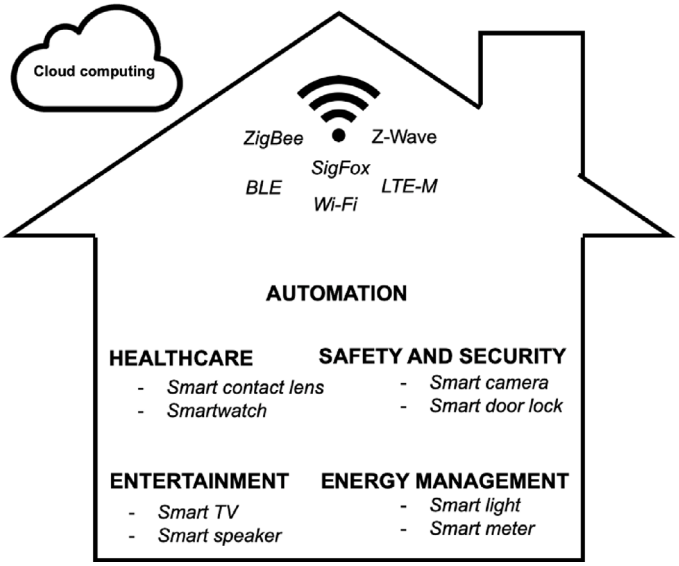


Fig. 2. An overview of a smart home.

3.3. The role of automation in smart homes

Automation is an essential part of the smart home. It consists of interconnecting many IoT devices and centralizing the remote control system. This configuration enables smart-home users to operate remotely home devices using the Internet and a terminal such as a smartphone. The interested reader in the IoT framework for smart-home management systems is advised to read these surveys [28,29].

3.4. Security requirements of the smart home

A smart home is a heterogeneous environment composed of devices, networks, software, and people, that requires different aspects of security which are described as follows.

Physical security and access control: Smart-home devices are vulnerable to physical access. Preventing unauthorized users from accessing or using these devices is a must.

Connectivity: A smart home often includes many IoT devices using different protocols, which could lead to security breaches. Ensuring the appropriate connectivity of smart-home devices is necessary.

Trust: Building trust in IoT transactions and increasing IoT trust should improve users' perception of safety and security in smart homes.

Software security: Smart-home users use various mobile apps to control IoT devices. Ensuring software security is necessary to prevent security breaches and data leakage.

IoT availability and service continuity: Smart homes provide users with services such as healthcare treatment that are critical. Therefore, another security requirement of the smart home relates to the availability and service continuity of IoT devices.

Network security: It is indispensable to deploy appropriate technologies to enable the resilience of smart-home networks and data security.

Privacy: The use of IoT devices at home increases the potential scenarios of privacy violations. Attackers can take advantage of smart-home devices to track users' activities and spy on them.

Cybersecurity awareness: Smart-home users should be aware of cyber threats and security hygiene to prevent cyberattacks.

4. Security issues in smart homes

Smart homes face many security issues for many reasons. First, these homes include various technologies (e.g., devices, networks, applications, cloud) that are not secure by themselves. Next, smart homes collect and process users' private information. Finally, home users usually have a low awareness of cybersecurity, and they do not have IT skills and knowledge like professional IT administrators to manage such a system. Overall, the combination of these issues from each component of smart homes involves many vulnerabilities, leads to an array of attacks, and complicates the design of defense [30].

4.1. Vulnerabilities of smart homes

In this section, we describe the critical vulnerabilities with respect to the components in smart homes.

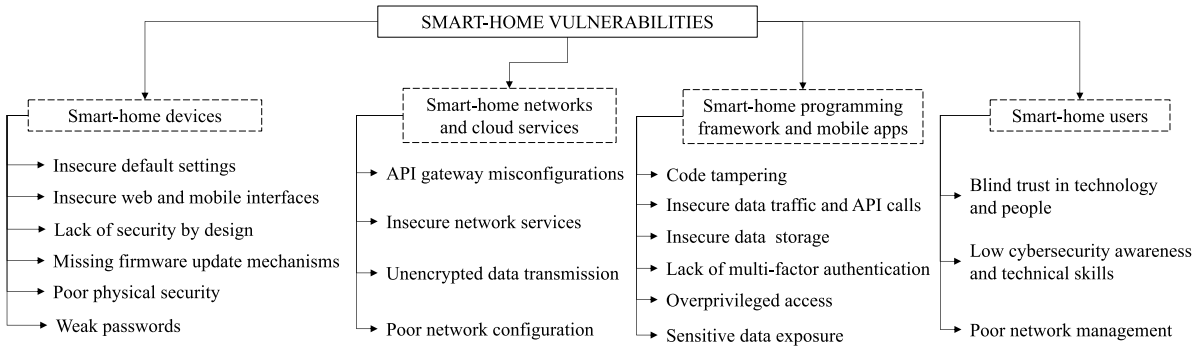


Fig. 3. Classification of the smart-home vulnerabilities based on its core components.

4.1.1. Smart-home devices

One major security issue in smart-home devices is the poor quality of IoT devices' security designs. Each layer of IoT devices suffers from many security issues [31,32]. First, the perception layer, which is responsible for data gathering, is vulnerable to attacks (e.g., eavesdropping, spoofing, and skimming) that can illegally modify or read the gathered data. Second, the network layer, which is responsible for the communication between the perception layer and the application layer, has the same vulnerabilities as available in the traditional network (e.g., Bluetooth, Wi-Fi, 4G, and 5G). Thus, cyberattacks, such as DDoS and sniffing, could cripple the network. Third, the application layer, which is related to the services offered by the device, can be subject to multiple cyberattacks such as Structured Query Language (SQL) injection and buffer overflows. A smart-home hub is a typical example of home devices. It connects IoT devices to the smart-home networks and manages them through a web interface or a mobile application. Recently, a study performed by Cisco Talos on Samsung SmartThings hub disclosed some vulnerabilities that could be exploited to compromise the security and privacy of smart-home users [33].

4.1.2. Smart-home programming frameworks

Emerging smart-home programming frameworks (e.g., Samsung's SmartThings, Apple's HomeKit, Google's Weave/Brillo) allow developers to build useful smart-home applications for end-users. However, those frameworks may expose smart-home users to significant security risks. In [34], the authors study the security analysis of the Samsung SmartThings framework. After investigation, they discovered two security–critical vulnerabilities. First, 55% of applications (SmartApp) built on this framework were overprivileged, whatever the level of authorization needed. Second, events generated by IoT devices could be spoofed since unprivileged apps could read all the activities of any devices. Moreover, in [35,36], the authors detected some vulnerabilities allowing unauthorized remote access to Apple's HomeKit.

4.1.3. Smart-home networks and cloud services

In smart homes, the network layer includes the communication between IoT devices themselves, IoT devices and the gateway, and the gateway and cloud services. Therefore, each sub-network of this ecosystem should be secure enough to guarantee the security and privacy of data transmission. As smart-home networks have an internal part and an external one, they constitute a potential access point for adversaries. In [37], after studying a few smart-home devices on the market, the authors find some vulnerabilities in network communication. For instance, they found that data exchange between the smart light bulb and the bridge were not encrypted, and they also got access to a smart camera illicitly by performing a MITM attack.

4.1.4. Smart-home users

Users play an essential role in the smooth running of technological systems (e.g., a plane and the pilots). Regarding information security, the human factor is also crucial. For instance, in [38,39], the authors describe the correlation between human factors and the lack of security awareness in any IT organization. Thus, users without security education may keep a hole in the smart-home security.

Fig. 3 shows four-dimensional vulnerabilities in the smart-home based on its core components. For more details regarding IoT device vulnerabilities, the interested reader could refer to the recent report of Open Web Application Security Project (OWASP) [40].

4.2. Attacks on smart homes

This section presents attacks on smart homes in three levels. First, we describe traditional cyberattacks, then we describe specific cyberattacks in smart homes, and lastly, we describe the other attacks that could occur in a smart home.

4.2.1. Traditional cyberattacks

In smart homes, the gateways, usually located at the edge of the home network, bridge the Internet and the local area networks (LANs). By doing so, the home network is accessible from the Internet. Thus, traditional cyberattacks (e.g., DoS attacks, side-channel attacks, eavesdropping) endanger smart homes.

DoS attacks: The primary goal of a denial of service (DoS) attack is to make resources (network, devices, applications) unavailable. When this attack occurs, users cannot access services anymore. A more sophisticated variant of this attack, i.e., Distributed DoS (DDoS), leverages compromised machines around the world to overwhelm the network traffic of a specific target. As a result, the target becomes unable to guarantee the continuity of services. Every year many DDoS attacks target network resources (e.g., servers) through the Internet. Thus far, the biggest one, with a peak of 1.35 Tbps, occurred in February 2018 in which the target was GitHub, a platform for developers community [41]. While this attack did not involve IoT devices, the second biggest DDoS attack to date did. In October 2016, more than 100,000 IoT devices, including those of smart homes (e.g., baby monitors, smart TVs, smart cameras), were hacked by Mirai malware for performing a DDoS attack on Domain Name System provider, Dyn [42].

Eavesdropping attacks: This attack, also known as sniffing or snooping attack, consists of monitoring the smart-home network in promiscuous mode and illicitly to get more information on the target. In this scenario, it is usually tricky to detect the presence of attackers. As an illustration, the authors in [43] describe an attack scenario in which attackers can eavesdrop on network traffic (encrypted or not) based on the ZigBee technology, a wireless personal area network (WPAN) designed for low power devices and used for IoT and smart-home networks.

Man in the middle (MITM) attacks: The scenario of this attack usually involves three entities. These include two legitimate users that communicate together and an illicit user that interferes in that communication without anyone noticing. The illicit user performs the attack by either eavesdropping on the conversation and getting the needed information or listening and capturing data from a legitimate user, then modifying that data and sending it to the other authorized users. Kang et al. [44] investigate data tampering by MITM attacks in IoT networks.

Traffic analysis: This attack consists of analyzing network traffic (encrypted or not) to discover useful information. As mentioned in [45], the traffic metadata analysis can allow an attacker to obtain confidential information on smart-home users, so that threatens users' privacy.

Replay attacks: This attack is part of MITM attacks since a replay attack allows an adversary to capture legitimate traffic (encrypted or not) and send it again by pretending to be an authorized user. Replay attacks are frequent in the traditional network as well as in IoT networks [43,46].

Masquerading attacks: In this attack, adversaries leverage legitimate users' credentials. They carry out masquerading attacks by using a forged identity to gain unauthorized access to the home networks so that they can manipulate user traffic data, system control data, and general user data [47].

4.2.2. Specific cyberattacks on smart homes

This section describes cyberattacks on smart homes with a focus on voice controllable systems (VCS). VCS, also known as smart speakers (e.g., Amazon Echo, Apple HomePod, Google Home, Sonos One), allow users to interact with other IoT devices of the home networks through voice commands. This device plays an essential role in the success of smart homes. As a critical component of smart homes, many cyberattacks have started to target VCS. In [48], the authors survey the recent acoustic cyberattacks on IoT devices, including VCS. Acoustic sounds may be inaudible to humans at specific frequencies (i.e., infrasonic sounds: $f < 20$ Hz; ultrasonic sounds: $f > 20$ kHz). As mentioned by the authors, attackers can leverage ultrasonic sounds to perform attacks (e.g., eavesdropping, denial of service, message forging) on VCS and threaten the privacy and security of smart-home users.

In [49], the authors describe the current attacks and defense techniques about VCS. These attacks consist of generating a signal that leads a VCS to execute a specific malicious command that the user cannot detect or recognize. Based on the type of implementation, the authors classified the attacks on VCS into three major groups. The first group of attacks (e.g., A11y attacks, and GVS attacks) exploits operating system vulnerabilities to make the attack self-triggered and more inaudible. The second group of attacks (e.g., Dolphin attacks, and IEMI attacks) is related to the hardware. Adversaries replay a synthetic non-speech analog signal instead of a human voice. The analog (inaudible) signal is carefully designed to match the characteristics of the hardware (e.g., the analog–digital converter). Thus, this inaudible signal can be converted into a legitimate digital speech signal by the hardware. The third group (including Speech Adversarial Example, and Hidden Voice Command) concerns the machine learning (ML) level attacks. Manufacturers equip most of VCS with automated speech recognition (ASR) based ML to convert digital speech signal to text. Given that ML, especially Deep Neural Network-based models, are vulnerable to adversarial examples' attacks [50], adversaries can compromise VCS.

Moreover, as discussed by Zhang et al. [51], virtual personal assistants (VPA), such as Amazon Alexa and Google Assistant, used by VCS, are not secure at all. When the VPA does not have the response to the user request, it asks a third-party app providing the required service to respond to that request. The third-party apps, which are usually called "skill" by Amazon and "action" by Google, could also be developed by hackers to compromise the VCS. In such a way, the authors executed a voice squatting and a voice masquerading attack based on malicious skills to compromise users' privacy. In a related study, Kumar et al. [52] perform a skill squatting attack on Amazon Alexa. The authors present some issues in Alexa speech-recognition system that can generate interpretation errors, and adversaries can leverage those errors and carry out cyberattacks on the smart speaker and users. In addition to acoustic-based cyberattacks, VCS are also vulnerable to light commands. In [53], the authors inject laser-based audio commands into VCS (e.g., Amazon's Alexa, Apple's Siri, Facebook's Portal, and Google Assistant) to get full control over these speakers that do not have any authentication systems. This attack is not noisy and could be performed on long distances (up to 110 m).

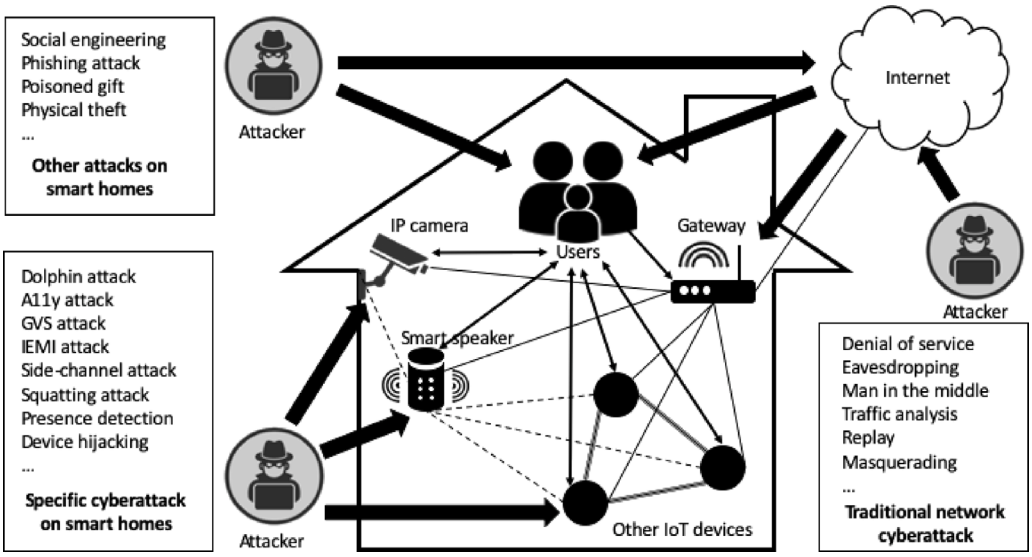


Fig. 4. An overview of cyberattacks on a smart home.

Another particular smart-home attack is depicted in [54] in which Patel et al. focus on the privacy of users inside smart homes. The authors leverage heating, ventilation, and air conditioning (HVAC) systems to detect human movements in the smart home. In that case, attackers could spy and compromise the physical security of users and their homes. Moreover, most baby monitors (smart cameras used to monitor babies remotely) have weak passwords or no password [55]. Since they are easy to hack, attackers have a particular interest regarding these security cameras. As stated in [56], after hijacking baby monitors of individuals, attackers talked through and threatened home users directly.

Finally, side-channel attacks can belong to those specific attacks. Standaert [57] defines side-channel attacks as "a class of physical attacks in which an adversary tries to exploit physical information leakages such as timing information, power consumption, or electromagnetic radiation". In a nutshell, side-channel attacks collect any external information on a running system, then perform reverse engineering based on this information to access more deeply to that system. Regarding smart homes, attackers could aim at exploiting IoT devices to collect sensitive data based on the internal operations of these devices. In [58,59], the authors describe side-channel attacks, e.g., electromagnetic attacks [60] and Fingerprint and Timing-based Snooping (FATS) attacks [61], on smart homes. The authors classify these attacks into two groups: the passive attacks when those attacks consist only in exploiting the output of systems, and the active ones when the execution of those attacks consists of modifying the state of the target system in input, and collecting and analyzing the system output.

4.2.3. Other attacks

In this section, we outline the potential attacks on smart homes that are not directly concerned by the two classifications mentioned previously. As reported by Alexander Pope, "To err is human, to forgive, divine [62]". Since home users are not sufficiently aware of IT security, they constitute a real issue in the security of smart homes. Nowadays, social engineering is a powerful tool used by attackers to imperil the security and privacy of home users. In December 2015, a cyberattack based on phishing email allowed cybercriminals to get access to the business network of an electricity infrastructure of Ukraine. As a result, power outages affected up to 225,000 homes for a few hours [63]. Moreover, the authors in [64] present a phishing attack in a smart home. In the proposed scenario, an attacker, which has gained control of a smart meter cloud-based services platform, sent a software upgrade request to a home user with a malicious link. Consequently, a home user who is not aware of this kind of threat could respond to this request and be hacked. As referred by Denning et al. [30], attack scenarios in smart homes are various and significant. For instance, users can purchase infected devices or receive them as a gift. In both cases, these corrupted devices could compromise the entire the smart-home security. From this angle, the authors in [65], after studying the external attack surface of a smart car, figured out how to compromise the vehicle via a corrupted compact disc (CD). Furthermore, Sivaraman et al. [66] demonstrate how intruders could infiltrate a smart-home network and perform several cyberattacks by leveraging a malware-based doctored smartphone application.

As described above, smart homes face many security issues. Fig. 4 presents an overview of potential cyberattacks on a smart home. The proposed home comprises an IP camera, a smart speaker, and other interconnected IoT devices, which are connected to the home network through the gateway. Home users can either directly interact with each device or send voice commands to the smart speaker to communicate with every IoT device of the smart home. We categorize the cyberattacks into three groups. Initially, the "traditional network cyberattacks" are related to the common network attacks such as DDoS, eavesdropping, MITM. Then, the so-called "specific cyberattacks on smart homes" concern those that target home-based IoT devices that collect information on home

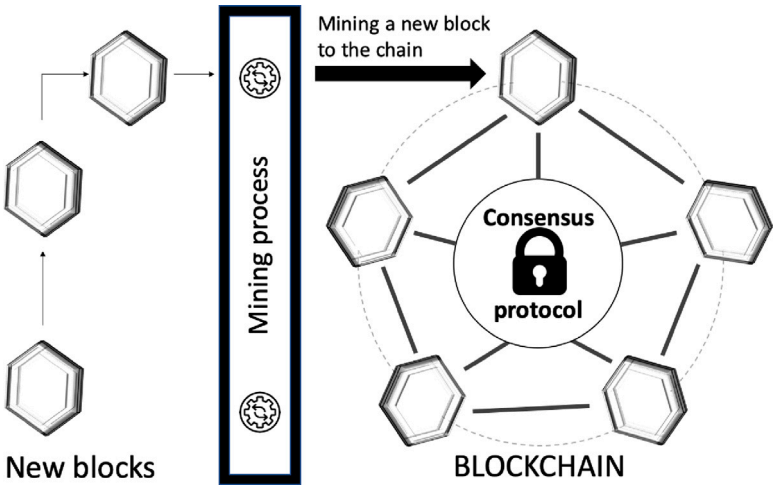


Fig. 5. An overview of the blockchain technology.

users. An example could be an attack that detects whether there is someone in a home or not. Lastly, the "other attacks on smart homes" describe the passive attacks, including social engineering and phishing attacks, that leverage the human factor, as a central entity in the smart home, and main vulnerability.

The following sections discuss how blockchain, SDN, and NFV could enhance the security of smart homes.

5. Technology solutions for smart home security

This section describes three technologies that could improve the security of the IoT and smart homes. The properties of each technology are unique and could constitute a possible solution regarding the security issues depicted in Section 4.

5.1. Blockchain

Although Satoshi Nakamoto [67] initially developed blockchain in 2008 for the decentralization and the security of electronic transactions (Bitcoin), the potential benefit of this technology is applicable in various fields, including science, economy, politics, and humanitarianism for addressing real-world problems [68]. Based on its main characteristics (decentralization, persistency, anonymity, and auditability) [69], researchers in IoT security leverage blockchain technology as well. A recent review concerning IoT performance and security requirements confirms this trend [70]. Fig. 5 illustrates the main concepts and paradigms of blockchain technology.

This technology is a distributed ledger-based on a chain of blocks. Each block contains a timestamp, a transaction (main data), the hash of the previous block, the hash of the current block, and other information [71]. The new blocks are added to the chain in linear and chronological order by the mining process. There are three types of blockchain technologies (i.e., public, private, and consortium blockchains).

- *Public blockchains*: They are permissionless. Any node can access to the network and process the blocks. Transactions are secure, transparent, and anonymous. Bitcoin and Ethereum are typical illustrations of public blockchains.
- *Private blockchains*: They are permissioned. Only authorized nodes can process the transactions. The nodes are limited, and it is easy to manage their identity. Private blockchains are faster and require little time and energy to validate transactions. There are many private blockchains, including Hyperledger Sawtooth and Hyperledger Fabric.
- *Consortium blockchains*: They are hybrid blockchains closer to the public ones. There is no access restriction to the network. However, only a group of the pre-approved networks can participate in the mining process. Corda and Hyperledger are typical examples of these blockchains.

5.1.1. Mining

Mining is the process of adding a new block into the blockchain. Miner nodes perform the mining process by solving a cryptographic puzzle. The miners are the nodes (single elements of the network) responsible for executing the mining process.

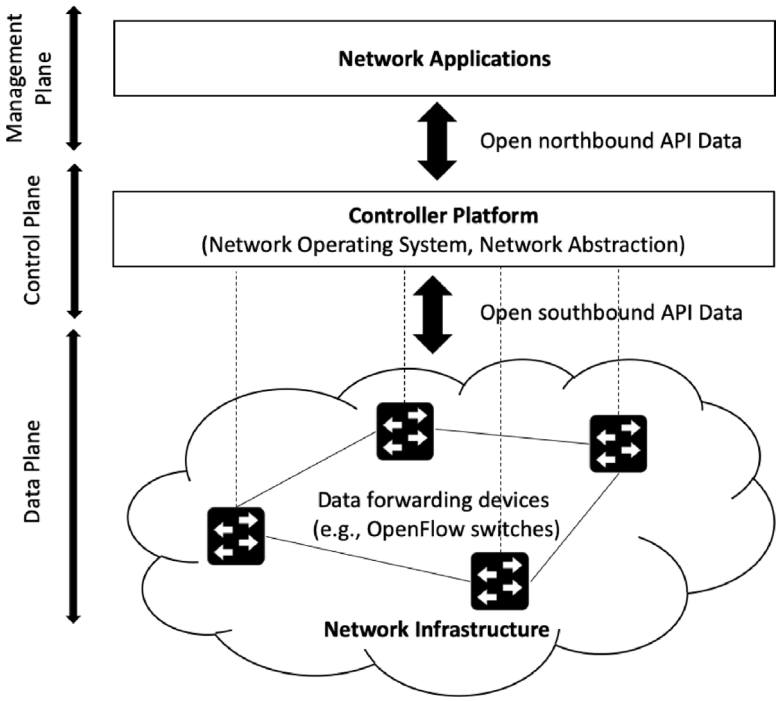


Fig. 6. An overview of a simplified architecture of SDN.

5.1.2. Consensus protocol

This mechanism makes all blockchain nodes have an agreement in the same block. Consensus protocol also ensures that the latest block has been added to the chain correctly, guarantees the integrity of transactions, and can protect from malicious attacks [71]. The consensus protocol is an essential concept of blockchain technology. Note that the consensus and the mining process go together. The most well-known consensus methods include the Proof of Work (PoW), the Proof of Stake (PoS), and the Practical Byzantine Fault Tolerance (PBFT). In [72], the authors provide an in-depth description of these concepts.

5.1.3. Smart contracts

Far from being a legal document, it is a concept introduced by the researcher Nick Szabo in 1994. Smart contracts are just transaction instructions (scripts) stored onto the blockchain. They can execute a specific instruction independently and automatically, depending on the occurred event [73].

5.2. SDN

Software-Defined Networking (SDN) is an emerging network management architecture. SDN is dynamic, manageable, cost-effective, and adaptable to deal with the high-bandwidth, dynamic nature of today's applications. This architecture decouples the network control and forwarding functions; thus, enabling the network control to become directly programmable and the underlying infrastructure to be abstracted for applications and network services [74].

SDN provides new techniques to solve many limitations (e.g., operating and hardware costs, network misconfigurations, and related errors) of current network architectures, especially by separating the control plane from the data plane [75]. As illustrated in Fig. 6, an application programming interface (API) (e.g., OpenFlow) could perform this separation. This figure presents the three core planes of a simplified architecture of SDN. Lastly, SDN transforms static networks into highly-programmable and adaptable networks. Thus this technology provides many advantages to the system, such as robustness, flexibility, performance, availability, scalability, manageability, and security. Although we outline the fundamental notions related to SDN below, the reader who is interested in a deep understanding of this technology could refer to the study of Kreutz et al. [75].

- *OpenFlow:* It is one popular application of SDN principles [76]. OpenFlow provides an open protocol that controls applications at the edge of the networks and access to resources such as routers and switches. McKeown et al. [77] describe the specifications of OpenFlow and show that it is possible to program the flow-table in various switches and routers through OpenFlow.
- *Data forwarding devices:* Any devices (hardware or virtual) that perform network operations related to packet manipulation and forwarding [78].
- *Data plane:* This plane is responsible for forwarding the traffic through interconnected devices such as routers and switches.

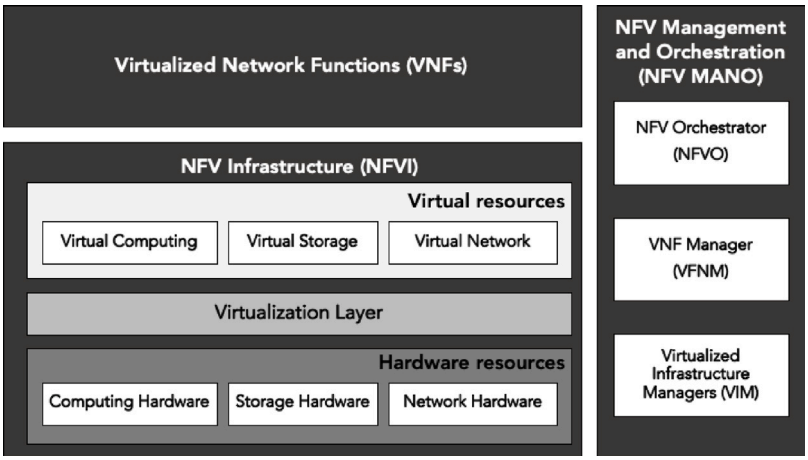


Fig. 7. An overview of a simplified architecture of NFV.

- *Control plane:* Part of the network in which all control logic (e.g., management of network devices and traffic) is performed.
- *Management plane:* This plane is responsible for monitoring, configuring, and maintaining network devices. It includes various applications that leverage the services delivered by the Northbound API.
- *Northbound API:* This interface is provided by the Network Operating System (SDN controllers) for developing applications. Located between the SDN controller and the network application, "the Northbound API presents a network abstraction interface to the applications and the management systems at the top of the SDN stack, and is hence considered to be the most important component of SDN Architecture [79]".
- *Southbound API:* This interface is used to establish the communication protocol (e.g., OpenFlow, NETCONF) between the SDN Controller and the lower-level components (data forwarding devices).

5.3. NFV

Network Functions Virtualization (NFV) can be defined as the concept of transferring the network functions from dedicated hardware appliances to software-based applications [80]. Thus, NFV is an IT virtualization technology that replaces network nodes such as routers, load balancers, intrusion detection systems (IDS), and firewalls into software running in virtual machines. By doing so, the network administration and management become more flexible, agile, and affordable. Fig. 7 presents a simplified architecture of NFV. A detailed architecture is accessible in [81]. The proposed architecture comprises three main blocks, including NFV Infrastructure (NFVI), Virtualized Network Functions (VNFs), and NFV Management and Orchestration (NFV MANO).

- *NFVI:* This block is an essential element of NFV. It provides the hardware and software resources needed to deploy the VNFs. NFVI comprises three components: the hardware resources (i.e., computing hardware, storage hardware, and network hardware), the virtualization layer, which creates a virtual occurrence of the hardware resources, and the virtual resources (e.g., virtual computing, virtual storage, and virtual networks).
- *VNFs:* They are the traditional network services (e.g., switching, load balancing, and routing) that are deployed as software services.
- *NFV MANO* This block aims to manage the NFVI and orchestrate the allocation of resources needed by the network services and VNFs [82]. NFVO orchestrates the NFVI resources across multiple virtualized infrastructure managers (VIMs) and manages the lifecycle of network services. VNFM manages the lifecycle of VNF instances. VIM is responsible for NFVI resources management.

6. Blockchain aware security solutions

In this section, we give more details on how blockchain could strengthen the security of IoT and smart homes.

6.1. Blockchain-based IoT security

The section is aiming to present the significant contributions of blockchain in IoT security through some use cases.

Table 3
Contribution of blockchain in IoT security.

IoT without blockchain	IoT with blockchain
Unreliable data	Data integrity
Weak or no encryption	Strong end-to-end encryption
Weak communications protocols	Robust communication protocols
Weak or no passwords	Strong identification
Weak or no access control	Strong data encryption
Side-channel attack vulnerabilities	Secure key provisioning
Hackable device keys	Multi-layer security
Non-trusted firmware	Trusted firmware
Weak Operating Systems	Strong/tested application
Untested third-parties plugins	Strong Operating Systems

6.1.1. Privacy, robustness, scalability, and security

These properties are included in the most recommended IoT requirements, and the blockchain technology may improve the IoT security through these properties. In [83], the authors leverage Bitcoin to secure the transaction in a decentralized smart grid. Initially based on a trusted third party, the traditional energy trading has many security concerns, including privacy and anonymity. Therefore, the system is exposed to cyberattacks, such as MITM attacks. Furthermore, traditional architecture is centralized and presents a single point of failure that could be abused by DDoS attacks. For this reason, the authors propose a system based on the blockchain, multi-signatures, and anonymous encrypted message propagation streams to provide privacy and security against the above-mentioned cyberattacks and other attacks such as Byzantine failures and double-spending attacks. The authors in [84] propose a security framework in smart cities based on blockchain. The proposed framework consists of four layers. From the bottom to the top: the physical layer, communication layer, database layer, and application layer. Note that the authors use a blockchain Ethereum in the second layer and a distributed ledger in the third layer. This framework provides many advantages, such as reliability, scalability, and resilience. Also, in [85], the authors propose a blockchain-based hybrid network architecture for smart cities to face IoT big data issues such as high latency, scalability, privacy, and security. In [86], the authors present how blockchain and smart contracts improve the robustness of IoT. As regards to its capacity to automate complex multi-step processes, smart contracts play a crucial role in any distributed peer-to-peer network. As seen in [87], smart contracts can guarantee the security of IoT data in a blockchain network.

6.1.2. Data integrity, trust and ID management

As described in [88], IoT devices firmware present many security issues. One way to address these issues is to keep the IoT devices firmware updated. In [89], the authors indicate that the current client–server model providing the latest version of firmware to IoT devices could be inappropriate for checking the firmware authenticity and validity. To cope with these challenges, the authors propose a new firmware update system that leverages blockchain technology. This system verifies the firmware version securely, validates firmware correctness, and downloads the most recent firmware. Furthermore, Ali et al. [90] provide an overview of various applications of blockchain in IoT security. The authors explain how blockchain can improve IoT security through trust, privacy, identity and data management, access control, data integrity, confidentiality, and availability. As described above, blockchain reinforces data integrity in IoT. Table 3 compares IoT environment with and without blockchain. In general, blockchains provide accessibility, incorruptibility, openness, and the ability to store and securely transfer data [91]. From now, we get more in-depth into the contribution of blockchain in smart-home architecture.

6.2. Blockchain-based smart-home security

In this section, we present the contributions of blockchain in the smart-home security, summarize, and compare the related works in Table 4.

6.2.1. Bitcoin for privacy, security and trust

Since IoT devices are resource-constrained and the blockchain is compute- and network-intensive, it could be challenging to implement the blockchain in smart homes. Hence, Dorri et al. [5] implement a lightweight blockchain for smart homes. The proposed architecture consists of three core tiers: a smart home, cloud storage, and an overlay network. There is no PoW, and only the smart home gateway is responsible for the mining process and the local storage. This framework addresses several smart home issues, especially data privacy and security, trust, IoT devices, and data management. It faces DDoS and linking attacks as well. However, the simulation generated some overheads, including packet overhead: 53 Bytes, time overhead: 20 ms, and energy consumption: 0.07 mJ. Furthermore, in [93], the authors propose an optimized blockchain that eliminates the overhead associated with the previous study while retaining its security and privacy benefits. The simulation results show a significant reduction in traffic and processing overhead. Another work [95] proposes a smart home community system based on blockchain. The system allows any trusted-smart home of the community to monitor the tracks and report the malicious activities occurring in another smart home, member of the community. The proposed architecture do not use the PoW and consists of home miners that collect transaction into a local and a community blockchain. The local blockchain is a private one, associated with only one smart home, whereas the community

Table 4
Comparative analysis of the selected works on blockchain and the smart-home security.

Ref.	Security goals	Targeted cyberattacks	Summary	Supporting technologies and tools	Key metrics or performances
[5]	Availability; Authorization; Confidentiality; Integrity; User control	DDoS attacks Linking attacks	Cope with high energy consumption and processing overhead by proposing a lightweight blockchain for use in IoT by eliminating the PoW and the concept of coins.	Bitcoin Cooja simulator [92]	Packet overhead: 53 Bytes Time overhead: 20 ms Energy consumption: 0.07 mJ
[93]	Accessibility; Anonymity; Authentication; Access control	DoS attacks; Modification attacks; Dropping attacks; Appending attacks	Introduce an architecture of blockchain-based smart home that uses distributed trust to reduce the block validation processing time.	Bitcoin ns-3 [94]	Traffic overhead: roughly 37 MB data (Current method) against 138 MB data (Traditional Bitcoin network); Processing overhead: reduction of processing time roughly by 50%
[95]	Availability; Authorization; Security alerts	Network attacks; DDoS attacks; Linking attacks	Propose a community of smart-home architecture where a smart home could interact with trusted external miners to identify unexpected and improper events.	Bitcoin	System responses for external events (e.g., access time delay, false alert, network failures, and power outages)
[96]	Privacy; Security	51% attacks; DDoS attacks; Mining attacks	Improve the storage capacity of blockchain for IoT devices and address network security issues (e.g., smart-home communication and access) using hyperedge for the organization of network nodes.	Bitcoin Hypergraph	Storage efficiency
[97]	Data security; Data availability; Computability and sharability; System robustness; Storage security	Network attacks	Propose a blockchain structure based on homomorphic encryption to protect data traffic in smart-home networks.	Hyperledger Fabric; Homomorphic encryption	N/A
[98]	Authentication; Authorization; Availability; Confidentiality; Immutability; Integrity.	N/A	Introduce a simplistic model of consortium blockchain for smart homes, which does not require cloud storage.	Consortium blockchain	Overall activity response time
[99]	Scalability; Availability; Security; Confidentiality; Integrity.	Network intrusion	Present a framework using cloud computing and blockchain for the smart-home security.	Amazon Elastic Compute Cloud; ZigBee; Cooja simulator; Netsim.	Network overhead; Throughput time overhead; Central Processing Unit (CPU) utilization; Receiver Operating Characteristic (ROC) curve; True Positive Ratio; False Positive Ratio.
[100]	Privacy; Scalability; Trust; Access control	N/A	Propose an architecture based on blockchain and smart contracts for the smart-home security.	Ganache [101]; Remix [102]; Web3.js [103] Ethereum; Smart contract	Access request
[104]	Immutability; Integrity; Security.	Modification attacks	Propose a blockchain-based framework to improve cybersecurity mechanisms in smart homes.	Smart contract; Ethereum.	Gas cost

(*continued on next page*)

Table 4 (*continued*).

[105]	Authentication; Availability; Confidentiality; Data privacy.	DoS attacks; Data mining and linkage attacks; Modification attacks.	Introduce a novel authentication system using attribute-based access control for smart-home users and devices.	Smart contract; Ethereum; Edge computing.	Block size; Gas cost; Time cost.
[106]	Availability; Authorization; Confidentiality; Identification; Integrity	N/A	Introduce an architecture to improve data security in smart homes.	Hyperledger Fabric; Smart contract	N/A

blockchain, which is also private, keeps records of the community transactions. Furthermore, this framework reinforces the security of smart homes, mainly by preventing malicious requests. However, the proposed model generates various packets overhead related to multiple events such as a power outage, network failures, and false alarms.

6.2.2. Hypergraph-based blockchain and consortium blockchain and for data security

Data security is a requirement in the smart-home security. Considering the constraints of low energy consumption, low computing power, and limited storage capacity related to IoT devices, the authors [96] use a hypergraph-based blockchain to reduce storage consumption and ensure data storage and security in smart homes. The proposed architecture presents a better storage capacity than the original blockchain. However, the accuracy of attack detection needs to be studied deeply. Other authors focus on consortium blockchain frameworks for the smart-home security. She et al. [97] use homomorphic encryption in blockchain to protect sensitive data and ensure user privacy in smart homes. Arif et al. [98] propose a cost-effective, secure blockchain to cope with extra overhead caused by traditional blockchain architecture. Moreover, Singh et al. [99] propose a secure and efficient smart-home architecture based on cloud computing and blockchain technology. They analyze network traffic and features to detect network intrusion.

6.2.3. Ethereum and smart contract for access control, data privacy, and trust

Privacy is a crucial issue for the smart-home security. In an effort to solve this problem, in [100], the authors use blockchain to improve data privacy in smart homes. They use Ethereum and smart contracts to achieve trust and access control. The proposed architecture consists of four entities: a service provider, storage devices, a smart home, and the homeowner (user). Furthermore, the authors introduce a compiling mechanism of three types of smart contracts, namely access control contract (ACC), judge contract (JC), and register contract (RC). Only the authorized smart-home user can create and manage the policy of the smart contracts. Through this policy, the homeowner can seamlessly remove or add IoT devices from the network. In case an intruder tries to perform a non-defined action inside the policy, this action is promptly canceled by the smart contracts, and the intruder has no longer access to the smart-home networks. Similarly, other papers have used Ethereum and smart contracts to create new frameworks for enhancing the smart-home security. Giannoutakis et al. [104] present a framework that registers smart-home users and IoT devices using smart contracts and analyzes the firmware integrity of gateways and IoT devices. In [105], the authors focus on an authentication scheme to improve access control in smart homes.

6.2.4. Hyperledger fabric and smart contract for integrity and security

Ensuring data integrity is still a challenge in the smart-home security. Therefore, in [106], the authors focus their research on how to leverage both smart contracts and blockchain to improve the integrity and security of IoT services in smart homes. The proposed architecture consists of three entities: the smart contracts, a local blockchain, and a public blockchain. The smart contracts define the communication and transaction rules among IoT devices. The local (private) blockchain manages the access control list (ACL) and smart-home devices. The public blockchain is a peer-to-peer (P2P) blockchain network that allows various smart homes to share data securely. The proposed architecture reinforces confidentiality, integrity, and availability of IoT data as well as identity proofing of homeowner and authorization procedure of IoT devices to join the smart-home networks.

Based on previous studies, it becomes evident that public, private, or consortium blockchain technologies and smart contracts contribute to the smart-home security through improved security, scalability, data integrity, privacy and trust, authentication, and access control.

7. SDN aware security solutions

In the following, we investigate how leveraging SDN could improve the security of IoT and smart homes.

7.1. SDN-based IoT security

As mentioned previously in Section 5.2, SDN embodies some solutions to improve the traditional networks. The same properties of SDN could reinforce the IoT network as well. Regarding IoT security, SDN could enhance five main points [21].

- *Traffic isolation:* The first point is related to the capacity of SDN to manage various network traffic employing a unique physical infrastructure securely and dynamically without any conflict of interest and protect the network from malicious requests [107,108].
- *Network security monitoring through centralized visibility:* The second point concerns the SDN controller. Indeed, as shown in Fig. 6, the Control Plane, which includes the SDN controller, has a broader view of the network infrastructure. Thus, implementing good security strategies in the SDN controller could help to analyze the network packets from the Data Plane (IoT devices) and detect any anomaly in the network [109–112].
- *Dynamic flow control:* The third point is related to the flexibility and manageability of SDN. SDN controller could be associated with other security systems, such as intrusion detection systems and intrusion prevention systems (IDS/IPS). As a result, this association could detect and prevent cyberattacks more effectively [113,114].
- *Host and routing obfuscation:* This point brings another piece of security to the IoT network. SDN reinforces data privacy and confidentiality via obfuscation that hinders adversaries from getting access to valuable information. In [115], the authors propose a system called "Black SDN" that enhances the security of IoT devices communication and hinders cyberattacks such as eavesdropping and packet injection. Furthermore, Latif et al. [10] propose a new routing protocol that uses blockchain and SDN to enhance IoT security.
- *Deployment of network security applications:* The last point focuses on an essential feature of SDN, namely, the network programmability. The idea consists of leveraging this functionality to deploy security applications. Frameworks such as OpenFlow security application development framework designed to facilitate the rapid design, and modular composition of OpenFlow-enabled detection and mitigation modules (FRESCO) [116] and OpenFlow Extension Framework (OFX) [117] support the development and deployment of security applications, including botnet and DDoS detection, on SDN.

7.2. SDN-based smart-home security

This section highlights the potential benefits that SDN could provide to the smart-home security. Table 5 summarizes and the main ideas discussed in this section.

Strengthening the security of the smart-home architecture: SDN may improve the architecture of smart homes. Sharma et al. [6] propose an architecture based on SDN applications and SDN programmable switches for securing smart homes. As a result, SDN allows the home network to be agile and flexible and ensures the communication between various IoT devices. The proposed architecture is expected to detect and mitigate cyberattacks such as DoS and DDoS attacks, prevent bursts on communication channels, and authenticate users' voice commands before sending them to the smart speaker for processing. In [118,119], the authors introduce a centralized smart-home network based on an SDN controller to fill the gap in the computing power of IoT devices and provide a lightweight authentication mechanism for preserving data privacy. Moreover, Wang et al. [120] present an SDN-based framework to enhance the network security of smart homes. They analyze thresholds of traffic behaviors on the control and data planes to detect anomaly behaviors.

Enhancement of firewall performances: The firewall monitors and analyzes the home-network traffic to authorize the legitimate traffic requests only and avoid any intrusion. However, this security system could not handle most existing attacks, especially those belonging to many-to-one or many-to-many categories [121]. In [122], the authors propose a solution based on SDN to fix horizontal port scans in smart-home networks. A horizontal port scan is a typical many-to-one attack in which adversaries look for vulnerable IoT devices by scanning many IP addresses on a single port. The authors propose an SDN-based firewall platform, including a cloud-based firewall controller and a local enforcer based on OpenFlow switches, that operates as a smart-home gateway. Accordingly, this solution increases the performances of firewalls so that they become able to detect and hinder horizontal ports scans.

Defense against forever-day vulnerabilities: Ge et al. [123] propose a strategy based on SDN to reinforce the security of smart-home devices. Since IoT devices could suffer from forever-day vulnerabilities, known vulnerabilities that are impossible to patch, the authors present two proactive defense mechanisms that leverage SDN to change the attack surface on the IoT network. These approaches consist of exacerbating and making harder the process of exploitation of IoT vulnerabilities.

Anomaly detection and mitigation: The smart-home network could be subject to cyberattacks, such as DDoS and network intrusion. To cope with this issue, in [126], the authors introduce a network-based intrusion detection and mitigation framework for securing the smart-home network. This framework utilizes SDN to reinforce the security and trustworthiness of the smart-home network, and OpenFlow controllers filter packets and prohibit illicit requests to access home devices. In the same vein, Gordan et al. [127] propose SDN-based architecture using Field Programmable Gate Arrays (FPGA)-based platforms for edge computing applications and K-Nearest Neighbor (KNN) for anomaly detection in smart homes. The proposed system is implemented using high-level synthesis (HLS). In [128], the authors propose a novel SDN architecture implemented with Open vSwitch (OVS) using Graphic Network Simulator 3 (GNS3) for the smart-home security. They use two Virtual LANs (VLANs) to distinguish between verified and non-verified IoT devices. In addition, they use ML models, i.e., KNN, Random Forest (RF), and Linear Kernel Support Vector Machine (LK-SVM), to classify IoT devices and detect anomalies in the smart-home network. Another framework is presented in [129]. The authors propose a dynamic and programmable DDoS detection system using SDN for the smart-home security.

It could be challenging for lay users to manage smart-home networks, including many IoT devices prone to cyberattacks. Previous studies showed that implementing SDN in the smart-home network brings a more flexible and robust network architecture that eases IoT devices classification, cyberattack detection and mitigation, and network management.

Table 5
Comparative analysis of the selected works on SDN and the smart-home security.

Ref.	Security goals	Targeted cyberattacks	Summary	Supporting technologies	Key metrics or performances
[6]	Authentication; Availability; Flexibility	DoS/DDoS attacks	Propose a smart-home architecture that prevents and mitigates network security attacks while reducing the cost of deployment and performance overheads.	iPerf [124] SDN	Prediction accuracy: 89.9% Prediction sensitivity: 91.1%
[118]	Anonymity; Authentication; Privacy.	Desynchroniza-tion; Eavesdropping; Replay attacks.	Propose an SDN-based architecture to centralize and secure the smart-home network.	SDN	Computation complexity; Computation time.
[119]	Confidentiality; Authentication; Anonymity; Privacy.	Modification attacks; Replay attacks	Propose an authenticated and privacy-preserving scheme using SDN for securing data transmission in smart homes.	SDN	Computation costs Computation time
[120]	Flexibility; Security	DDoS attacks	Use SDN to improve IoT network management and analyze traffic behavior-based thresholds to detect cyberattacks.	SDN	Detection rate: 99.9% Detection time (control plane): 0.5–3.7 s Detection time (data plane): 1–11.7 s
[122]	Scalability; Security	Horizontal port scans attacks	Introduce an SDN-based network-level firewall platform to detect and block horizontal port scans and protect the smart-home network.	Firewall FleXight [125] SDN	Detection accuracy: 99% Network overhead: 0.75%
[123]	Security	N/A	Propose proactive defense mechanisms to deal with non-patchable vulnerabilities IoT network.	SDN	Reduction of attack success probability (ASP); Increasing of mean-time-to-compromise (MTTC)
[126]	Flexibility; Security	Network intrusion	Introduce a network-based intrusion detection system to identify and address potential attacks on smart homes.	ML SDN	Linear logistic regression classification model (precision rate: 94.25% and recall rate: 85.05%); Nonlinear classification model (prediction rate: 98.53% and recall rate: 95.94%)
[127]	Processing efficiency; Security.	Network intrusion	Use SDN and ML to develop efficient network intrusion detection for the smart-home security.	FPGA; SDN; ML (KNN); HLS;	Latency of sorting algorithm; HLS resource usage; Detection accuracy.
[128]	Efficiency; Flexibility; Security.	DDoS attacks	Propose an SDN-based architecture deployable on a low-cost edge system, distinguish between verified and non-verified IoT devices, and detect anomalies in the smart-home network.	ML (KNN, RF, LK-SVM); OVS; SDN; VLAN.	Anomaly detection accuracy: 98% Device classification accuracy: 97%
[129]	Scalability	DDoS attacks	Present a framework that uses SDN to improve data transmission in IoT networks and dynamically detect DDoS attacks in a reasonable short time.	SDN	CPU utilization; Memory utilization; Network throughput; Controller workload; Attack detection time

8. NFV aware security solutions

As reported earlier in Section 5.3, the goal of NFV is to decouple network functions from dedicated hardware appliances. This characteristic provides new opportunities to reinforce the security of smart homes.

NFV could contribute to ensuring trustworthiness, high availability, safety, and security in smart homes.

Trustworthiness in identity management: When discussing security, trustworthiness is a requirement that encourages users to adhere to a system or not. In [130], the authors highlight the importance of the trustworthiness of cyber–physical mapping. They use NFV to create a unique (physical and virtual) ID of IoT nodes allowing the mapping of these nodes. Such a system could be crucial in many scenarios, including earthquakes or disasters, to identify IoT devices, then detect and ensure the safety and security of IoT users and people in general.

High availability: In an environment full of threats, such as DDoS attacks, IoT architecture should ensure the high availability of services. In [131], the authors propose an IoT-cloud architecture using NFV for the high availability of IoT-cloud services. The

Table 6
Comparative analysis of the selected works on NFV and the smart-home security.

Ref.	Security goals	Targeted cyberattacks	Summary	Supporting technologies	Key metrics or performances
[7]	Scalability; Security.	DDoS attacks	Introduce a network security monitoring system, which includes P2P communications of many smart homes at the ISP level.	GenieACS 1.1 [134]; MUD; NFV.	N/A
[130]	Identification; Safety; Trustworthiness.	N/A	Propose an NFV-based framework for ID-based location mapping of IoT devices to ensure location-based services in smart environments, e.g., a smart home.	NFV	N/A
[131]	Fault detection; Fault recovery; High availability.	N/A	Propose a multi-layer architecture using NFVI and NFV MANO to provide high availability for an IoT-cloud environment, e.g., a smart home.	OpenStack Tacker; NFV	Mean time between failures; Mean time to repair.
[133]	Security	Brute-force attacks; DoS attacks; ICMP attacks; Scanning attacks; SYN attacks.	Deploy security functions (VNFs) at the network edge to perform traffic analysis.	Docker [135]; iPerf; ML; NFV; Xerxes [136].	Known attacks detection accuracy: approximately 95% per second

proposed architecture is implemented with OpenStack, a cloud computing platform, and OpenStack Tacker, playing the role of a MANO. NFVI and NFVM are used to configure fault detection and fault recovery. The evaluation of that architecture presents an average availability of almost 99.80%. This performance highlights the significant contribution of NFV to reaching high availability in smart homes.

Security monitoring: It is essential to monitor the smart-home network to identify vulnerabilities, suspicious behaviors, or ongoing attacks. Afek et al. [7] use NFV and Manufacturer Usage Description (MUD) to monitor many home networks. Note that MUD is a system that allows manufacturers to provide patterns of IoT device communication to the local network administrator to reduce the attack surface on IoT devices [132]. In the proposed architecture, the authors deploy the system composed of NFV and MUD directly within the Internet service provider (ISP) network. Thus, the system receives a copy of the traffic from the point of presence (PoP) router located on the ISP side. Monitoring many smart-home networks from a central location (i.e., ISP) enables the proposed system to detect and mitigate DDoS attacks. In addition, the proposed system could accept or deny any packet from or to IoT devices that do not satisfy the MUD rules.

Deployment of security functions: Implementing network security functions becomes more manageable using NFV. Sairam et al. [133] propose NFV-based Edge Traffic Analysis (NETRA), a lightweight Docker-based architecture for VNFs, to fulfill the security of smart homes. Their experiments reveal that the Docker-based NETRA architecture provides better performances regarding storage, memory, latency, network, and scalability than a virtual machine (VM)-based Open Platform for NFV (OPNFV). NETRA enables the deployment of security-based VNFs, including Wireless Access Point (WAP), firewall, IDS, software-defined switch, and edge analytics, for the security of the smart homes. We summarize the findings in Table 6.

Traditional security equipment could be expensive and not convenient, e.g., physical space constraints, for smart-home users. NFV enables fast and affordable deployment of network security functions using a single device allowing more flexibility and reducing costs. We summarize the findings regarding the contribution of NFV to the security of smart homes in Table 6.

9. Hybrid security solution

This hybrid security solution combines blockchain, SDN, and NFV to reinforce the security of smart homes. In this section, we point out the advantages of the combination of these technologies for the smart-home security.

9.1. Blockchain/SDN in the smart-home security

As part of the enhancement of the smart-home security, Boussard et al. [137] consider the automation of the risk management system as an essential tool to allow home users, whatever their background, to be able to evaluate the security of their IoT devices by themselves. The authors address this challenge by designing an architecture that relies on intelligent SDN-based home network controllers and blockchain. The role of SDN is to simplify the home network management while blockchain reinforces trustworthiness by implementing a crowd-sourced device trust assessment system. IoT devices are grouped into isolated network slices managed by the home controllers. As a result, this architecture improves the security of smart homes by reducing attack surfaces and identifying and hindering malicious behavior in the home networks. Furthermore, this system allows home users to easily monitor the trust level (e.g., good, average, suspect) of their devices in real-time.

In [138,139], the authors propose different architectures that leverage SDN and blockchains to improve data analysis, security, and energy management in IoT networks. Although the researchers do not specify the targeted IoT applications of these architectures, we assume that smart homes could be potential use cases. Sharma et al. [138], aware of the issues in IoT networks such as flexibility, efficiency, availability, security, and scalability, propose an architecture called DistBlockNet, which leverages SDN and blockchain to address these issues. In this architecture, IoT forwarding devices are interconnected to controllers located in a distributed blockchain network. Each local network includes three components, specifically OrchApp, Controller, Shelter modules that address the security issues. OrchApp modules integrate security policies that focus on data protection and access control. Shelter modules have many functions. First, they monitor and parse the communication packets to identify the appropriate OpenFlow packets. Then they analyze the parsed OpenFlow packets to obtain the topological metadata and status of the transmission. Finally, they prompt an alarm signal when an untrusted entity tries to modify the current flow or when the current flow does not fit the security rules specified by the administrator. Controller modules manage the communication between OrchApp modules and Shelter modules. The evaluation of this system focuses on defenses performances against cyberattacks, accuracy rates, scalability, and overhead analysis. In a nutshell, the authors provide a framework that mitigates cyberattacks, such as cache poising/ARP spoofing, DDoS/DoS attacks, detects security threats, ensure data security and access control. Zeng, Zhang, and Xia [139] propose a blockchain-based SDN-enabled IoT network architecture to ensure secure routing among multiple domains. They use the concepts of local and global reputations to promote the routing reliability. Note that the global reputation is reserved in the blockchain. The performance evaluation of a testbed composed of Open Network Operating System (ONOS), Mininet, and Hyperledger Fabric to emulate IoT networks show that the proposed architecture can effectively build global trust between multiple controllers and secure routing reliability among several domains.

Moreover, in [140], the authors leverage distributed blockchain to ensure the security and reliability of IoT nodes in a smart home. These nodes are classified in different blockchains, depending on computational power. Each IoT node represents a block of the blockchain, and each blockchain is connected to each port of the virtual switch Open vSwitch (OVS), which is managed by the SDN controller. The purpose of the proposed architecture is to ensure the efficiency in proof-of-work and computational complexity, enhance data integrity, ensure the identity management of IoT devices, reduce the network latency, and reinforce the security of the system by implementing the Elliptic Curve Digital Signature Algorithm (ECDSA) as the cryptographic algorithm of the blockchain.

9.2. SDN/NFV in the smart-home security

The works in SDN and NFV are increasing in many dimensions, including IoT security projects. The two technologies are independent but complementary to each other, and their association (SDN/NFV) provides many advantages. Farris et al. [21] point out that compared to traditional IoT solutions, scalability is more effective when combining SDN and NFV.

In [9,141], the authors discuss how to defend the smart-home network against sophisticated intrusions. They propose a multi-stage attack mitigation mechanism for software-defined home networks that leverages SDN/NFV to monitor comprehensive network events and deploys NFVs instantly. As a result, the proposed SDN/NFV-based architecture contributes to assessing the security level of smart-home networks, deploying security functions, and mitigating cyberattacks.

[142], the authors introduce an SDN-based framework that improves the smart-home network management and access control. The proposed framework enables manufacturers to implement the least privileged policy for the IoT, security service providers to enforce dynamic and static access control at the smart-home network level, and users to specify the network policy of the smart home. Moreover, the authors use an NFV security service, e.g., IPv4 ARP server, to mitigate ARP spoofing and network scanning.

Lastly, SDN and NFV represent the core technologies of Advanced Networked Agents for Security and Trust Assessment in CPS/IoT Architectures (ANASTACIA) framework. This project, funded by the European Union, aims to conceive, develop, and demonstrate a holistic solution enabling trust and security by design for IoT [143]. Zarca et al. [144] design a security management architecture based on SDN and NFV for the ANASTACIA project. The proposed framework can automatically monitor, detect, react, and mitigate IoT attacks, enforcing proper security policies, in reasonable times.

As mentioned above, SDN and NFV technologies can improve IoT network security significantly. Thus, researchers are getting interested in these technologies to enhance the security of smart homes. Table 7 presents the findings regarding the previous work using SDN/NFV for the smart-home security. We note that SDN manages the traffic route while NFV creates a virtual network function of security systems. For example, in the case of IDS, NFV creates a Virtual IDS that analyzes the network traffic mirrored within SDN. These systems take advantage of more scalability and can handle many IoT security issues, including DoS attacks, Sybil attacks, and MITM attacks.

9.3. Hybrid solution for the smart-home security

Before discussing the content of this section, note that some authors, including Alvarenga et al. [146], show how blockchain could significantly address some vulnerabilities in NFV–for example, by securing the management, configuration, and migration of VNFs. However, thus far, in the literature, we have not found any work related to the unique association blockchain-NFV in the IoT security domain. Table 8 summarizes and compares the existing works based on multiple parametric features.

The current section presents an architecture describing a potential case of integration of blockchain, SDN, and NFV in a smart home. A recent work [11] that introduces the implementation of a distributed secure blockchain with SDN and NFV for the security and privacy of smart cities has inspired the proposed architecture of the smart-home security in Fig. 8. The proposed architecture consists of four layers. Layer 1 contains the interconnected smart-home devices. We represent these devices using small black circles

Table 7
SDN/NFV-based security systems for IoT security.

Security systems	SDN/NFV based security systems	IoT security issues
Intrusion Detection System (IDS)	Through a secure data tunnel, SDN mirrors the traffic to be analyzed by the Virtual Intrusion Detection System (vIDS).	DoS attacks; Flooding attacks; Sybil attacks; Abnormal network activities; Battery draining attacks; Selective forwarding attacks.
Firewall	By using a secure data tunnel, SDN routes the traffic through the Virtual Firewall (vFirewall).	Access control; Port scanning; DoS attacks; Fragmentation attacks; IP spoofing attacks.
Deep Packet Inspector	Through a secure data tunnel, SDN mirrors the traffic to be analyzed by the Virtual Intrusion Detection System (vIDS).	Spoofing attacks; Malicious code injection attacks; Malformed network packets; IP spoofing attacks.
Encryption	By using a secure data tunnel, SDN re-routes the traffic to be analyzed through the Virtual Encryption Proxy (vProxy).	MITM attacks; Eavesdropping attacks; Data alteration; Sniffing attacks; Impersonation attacks.
Authentication; Authorization.	SDN injects the flow rules for each authenticated IoT device, and NFV creates a virtual authentication, authorization, and accounting framework.	IoT authentication inter-working; Service logging failures; Access control; User activity tracking.
Security Service Function Chain (Security SFC)	While SDN manages the flows to and from the Security SFC using packet tagging, NFV creates multiple virtualized security systems (e.g., vFirewall, and vIDS).	A combination of security threats (depending on the security enablers which are part of the implemented service chain).

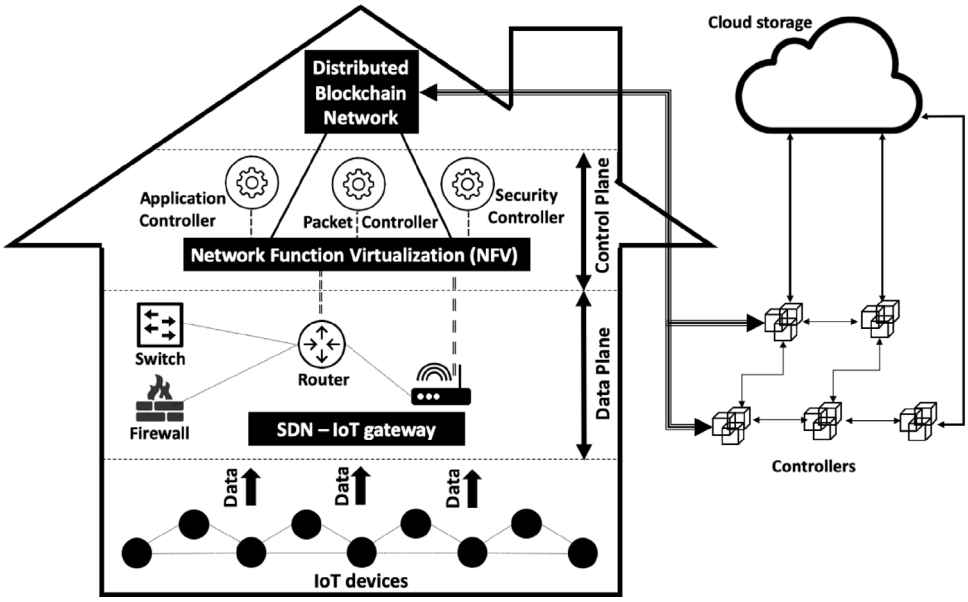


Fig. 8. An overview of blockchain, SDN, and NFV in a smart-home architecture.

linked by thin lines. The data generated by devices are centralized using an SDN-based IoT gateway located at the data plane. This data plane is part of Layer 2, managed by an SDN infrastructure that includes network devices such as a switch, a firewall and a router. The SDN controller ensures the security to the smart-home network by implementing the right security policies. Only the authorized data leaves the data plane to reach the control plane on Layer 3 where NFV is implemented. NFV virtualizes the data and specific VNFs, i.e., application controller, packet controller, and security controller, are used to reinforce the security of incoming and outgoing data traffic. Layer 4 contains a distributed blockchain network that takes advantage of the computation power of cloud computing to control data integrity. Using a decentralized blockchain in cloud computing reduces the operational costs and energy consumption of nodes, enables fault tolerance and high availability, and ensure data security.

The proposed framework uses blockchain to reinforce the robustness of the smart-home networks. Moreover, it could mitigate cyberattacks such as DDoS attacks and network intrusion by using SDN controllers and VNFs-based security systems. Although the integration of blockchain, SDN, and NFV could also significantly ameliorate security, privacy, confidentiality, integrity, availability, reliability in smart homes, an in-depth evaluation of the proposed architecture to determine the effectiveness and efficiency of this architecture is necessary.

Table 8
Comparative analysis of the selected works on BLOCKCHAIN-SDN-NFV and the smart-home security.

Ref.	Security goals	Targeted cyberattacks	Summary	Supporting technologies	Key metrics or performances
[9]	Availability; Confidentiality; Integrity.	Multi-stage attacks	Introduce a mechanism to evaluate the security of the home network, select the appropriate countermeasures, and mitigate multi-stage attacks.	NFV; SDN	Probability of attack path 1: 0.182 (before countermeasure) 0.018 (after countermeasure); Probability of attack path 2: 0.104 (before countermeasure) 0.010 (after countermeasure).
[11]	Availability; Accessibility; Confidentiality; Integrity; Privacy; Reliability.	DDoS attacks	Propose an architecture based SDN, NFV and a distributed secure blockchain for smart cities security.	Blockchain; NFV; SDN; Mininet	Throughput; Packet arrival rate.
[137]	Trustworthiness	Network attacks	Introduce a system that reduces the attack surface and automates risk assessing and management of IoT devices for users.	Blockchain SDN	Trust score
[138]	Availability; Access control; Data protection; Flexibility; Scalability; Threat prevention.	Cache poising ARP spoofing DDoS/DoS attacks	Propose an architecture that automatically updates the landscape threats, and generates and deploys the security countermeasures.	Blockchain SDN Mininet [145]	Efficiency and effectiveness of scalability, defense effects, accuracy rates, and performance overheads
[140]	Identity management; Data integrity; Reliability; Security	N/A	Propose a model to cope with IoT security issues, including low computational power, small storage capacity, and low-security level.	Bitcoin; Cooja simulator; ECDSA; SDN.	N/A
[141]	Security assessment	Attacks exploiting CVEs	Introduce a framework that assesses the smart-home network security and mitigates cyberattacks targeting known vulnerabilities.	SDN; NFV.	Costs of security countermeasures
[142]	Access control	Network scanning; ARP spoofing.	Propose an SDN-based framework to make access control more dynamic for the smart-home network and introduce an IPv4 ARP server as an NFV security service against ARP spoofing.	SDN; NFV; Data Plane Development Kit.	Bandwidth; ARP response time
[144]	Privacy	DDoS attacks IoT malware attacks	Present a security management architecture that aims to cope with security and privacy issues in IoT networks.	NFV; SDN	Incident handling performance; Monitoring performance; Reaction enforcement performance

A challenge related to the proposed architecture is whether it could ensure trust between the smart-home devices. As we can see, Layer 1 could need additional security systems to authenticate the identity of devices. However, enforcing control policies using SDN could solve this problem. Another challenge is related to the cloud server. It promotes a centralized architecture which involves more security issues than a decentralized architecture [147]. However, we suspect that implementing a decentralized blockchain in the cloud could alleviate these security issues, such as a single point of failure. Moreover, the choice of the type of blockchain technology to implement could be challenging, given that consensus protocols such as PoS, PoW, and PBFT generate different levels of performance, security, and energy consumption. Ultimately, future work should simulate and evaluate the performances of the proposed architecture for the smart-homes security.

10. Performance evaluation

Security performance evaluation is an essential step towards improving any system. This section describes evaluation tools, datasets, and metrics that one could consider to validate a proposed method for smart-home security solutions. Table 9 describes the performance evaluation of the cited papers in the previous comparative analysis.

Table 9
Performance evaluation of cited papers.

	Tools	Datasets	Metrics
[5]	Cooja simulator	N/A	Energy consumption; Packet overhead; Time overhead.
[6]	iPerf	SherLock dataset	Performance overhead (flow packet drop rate, flow setup time, and controller response time); System performance (processor, memory, and bandwidth).
[9]	Mechanism of evidence-driven security assessment using SDN factors and NFV-based detection	CVE-2015-0235; CVE-2009-1535; CVE-2008-3060; CVE-2008-5416; CVE-2007-4752; CVE-2004-0840; CVE-2003-0693.	Security level (the success probability of an attack path)
[93]	ns-3	N/A	Processing overhead Traffic overhead
[95]	N/A	N/A	Packet overhead
[96]	N/A	N/A	Storage capacity
[100]	Blockchain (Ganache, Remix, web3.js)	N/A	Access request
[106]	N/A	N/A	N/A
[122]	N/A	WITS:ISPDSL-II dataset	Network overhead; Visibility of the controller over active flows; Storage capacity; Accuracy of detecting attackers and identifying attack victims.
[123]	AKAROA2	N/A	Attack success probability; Attack impact; Attack cost; Mean-time-to-compromise Risk; Risk; Return-on-attacks; Mean-attack-path-length; Average shortest path length.
[126]	ML (Logistic regression, Non-linear SVM)	N/A	Precision; Recall
[7]	N/A	N/A	N/A
[133]	iPerf	N/A	Latency; Load average; Memory usage; Scalability; Storage; Throughput
[137]	N/A	N/A	Trust score
[138]	Mininet	N/A	Accuracy rate; Performance overhead
[140]	Cooja simulator	N/A	Bandwidth; Computing power; Memory capacity.
[144]	Cooja simulator	N/A	Monitoring performance; Incident handling performance; Reaction enforcement performance.
[11]	Mininet	N/A	Throughput; Packet arrival rate.

10.1. Simulation tools

There are many tools to simulate IoT and smart-home networks. We can make use of them according to purpose, scale, and so on.

AKAROA 2: It is a quantitative stochastic simulation using automated sequential analysis that can improve the credibility of results. Furthermore, it can speed up simulations using Multiple Replications In Parallel (MRIP) to harness the computing power of a network of inexpensive workstations [148].

Cisco Packet Tracer: It provides a variety of IoT components from version 7.2 upwards to build smart-home networks, including home gateway and IoT devices [149].

Cooja simulator: A network simulator that focuses on Wireless Sensor Networks. Cooja simulator is part of Contiki, an open-source operating system for the IoT [92].

CupCarbon: It is a multi-agent and discrete event simulator for wireless sensor networks based on OpenStreetMap. The multi-agent simulation parallelizes the behavior of sensors and makes them independent, and the discrete event simulation simulates data transmission between sensors [150].

GNS3: Graphic Network Simulator 3 (GNS3) is a network simulator and emulator that offers a risk-free virtual environment to build, design, and test (IoT) networks [151].

iFogSim: A tool for modeling and simulating IoT and Fog environments and measuring the impact of resource management techniques in terms of latency, network congestion, energy consumption, and cost [152].

IoTIFY: A cloud-based IoT system simulation platform that enables large-scale and realistic deployment of IoT solutions [153].

IoTNetSim: A tool that models and simulates end-to-end IoT services with a detailed representation of IoT systems and services, i.e., starting from the data sensing phase to data analysis in the cloud [154].

IOTSim: An IoT simulator enabling IoT big data processing using the MapReduce model in a cloud computing environment [155].

iPerf: A testing tool that analyzes and measures network performance based on many parameters such as bandwidth and lost datagrams [124]. iPerf measures many metrics, including latency, memory usage, and throughput, that matter for the smart-home security.

MIMIC IoT Simulator: A suite of simulators that can be used to build a real-world test lab and simulate an IoT environment such as a smart home [156].

Mininet: A network simulator that provides information on systems behaviors and performances. Mininet runs real kernel, switch, and application code on a single machine (VM, cloud, or native) and supports SDN and OpenFlow [145].

Netperf: A network performance benchmark that provides tests for both unidirectional throughput, and end-to-end latency [157].

NetSim: A network simulator and emulator that can be used to evaluate IoT network performances [158].

ns-3: A discrete-event network simulator for Internet systems [159]. ns-3 supports sensors and IoT network simulations [94].

OMNeT++: A network simulation environment whose model structure consists of modules that communicate with message passing [160]. Objective Modular Network Testbed in C++ (OMNeT++) includes many functionalities such as supporting sensor networks, wireless ad-hoc networks, Internet protocols, and performance modeling [161].

OPNET: Optimum Network Performance (OPNET) is a network simulator that emulates the behavior and performance of any networks, including wireless sensor network and IoT [162,163].

SimIoT: An IoT simulator focusing on data processing in a cloud environment [164].

For the interested readers in the simulators mentioned above, we suggest the following survey [165]. Furthermore, we advise those interested in 3D smart-home simulators to refer to [166,167], and [168].

10.2. Datasets

In [6], the authors used the SherLock Dataset to perform their analysis. SherLock dataset [169] is a smartphone dataset obtained from 50 users over a few years. This dataset contains billions of data records (e.g., call/SMS log, location, network stats, and running applications). It has many usages in cybersecurity, including malware detection and application profiling, malware analysis, continuous user authentication, context-based security, security-related statistics, and feature monitoring and extraction. In [9], the authors focused on the Common Vulnerabilities and Exposures (CVE). CVE [170] includes many publicly disclosed cybersecurity vulnerabilities and exposures. When proposing a new information channel to protect home user devices with an SDN-based firewall, Shirali-Shahreza and Ganjali evaluated their method on WITS: ISPDSL-II dataset [171].

Generally speaking, one may use synthetic data, testbed data, or benchmark data to validate a proposed smart-home security solution. Researchers may generate synthetic data for smart homes using open source tools such as OpenSHS [172], SHIMA [173], and SESim [174]. Another option consists of building a testbed environment consisting of sensors and smart-home devices to capture real time traffic. Finally, researchers may use public benchmark datasets such as UNSW-NB15 dataset [175], NbaIoT [176], Bot-IoT dataset [177], IoT-23 dataset [178], and TON_IoT dataset [179].

10.3. Metrics

Smart-homes security involves several key metrics, including energy consumption, packet overhead, storage capacity, performance, and throughput. Table 9 provides a summary of the performance evaluation methods of the related works discussed in this paper. Almakhdhub et al. [180] propose a benchmark framework that introduces 14 metrics: eight security metrics (i.e., total privileged cycles, privileged thread cycles, system call cycles, maximum code region ratio, maximum global data region ratio, data execution prevention, number of available Return-Oriented Programming (ROP) gadgets, number of indirect calls), two performance metrics (i.e., total runtime cycles, sleep cycles), three memory metrics (i.e., total Flash usage, stack and heap usage, total Random Access Memory (RAM) usage), and one energy metric (i.e., total energy consumption), for IoT microcontrollers. Dinh and Lim [181] focus on two network performance metrics: end-to-end delay and frame reception ratio. As for Savola et al. [182], they analyze the security risks in IoT-based e-health systems and describe some security metrics categorized into two security objectives: availability and configuration correctness.

10.4. Instruments for specific cyberattacks on smart homes

This section provides researchers with attack source codes regarding the specific cyberattacks on smart homes we described in 4.2. We encourage researchers to use these codes only to advance scientific knowledge and approaches towards ensuring the security and safety of smart-home security and users.

Dolphin attack: Researchers could implement this attack using a benchtop or a portable setup. The setup consists of an audio signal source, signal generator, ultrasonic speaker, audio amplifier, and ultrasonic transducer [183].

A11y attack: It refers to attack paths that target accessibility features of hardware and software such as operating systems. An experimental setup and code of A11y attack are accessible in [184].

GVS attack: Google Voice Search (GVS) attack is an attack on voice assistant modules that can forge SMS/Email, access private information, transmit sensitive data and achieve remote control without any permission. An illustration of attack setup and implementation are explained in [185].

IEMI attack: Wireless or hardwired, Intentional Electromagnetic Interference (IEMI) attacks could compromise smartphones and IoT devices and enable attackers to intercept and decrypt sensitive information. An experimental setup of this attack is detailed in [186].

Side-channel attack: It is an attack that exploits indirect measurements of a computation system and aims to exfiltrate sensitive information. There exist many security test labs and tools [187], researchers can explore to propose appropriate security countermeasures.

Squatting attack: Attackers can use squatting attacks on smart speakers by building malicious programs. Algorithms and attack flow to implement this attack on Alexa Skill are described in [188].

Presence detection: Detecting human activity and physical presence in a smart home can be useful to ensure users' security and safety. A presence detection algorithm detailed in [189] can support future research.

Device hijacking: Researchers can use many tools to investigate vulnerabilities of IoT devices and propose security solutions to prevent attackers from being able to control users' devices. CyberSecurityUP [190] provides a non-exhaustive list of these tools which researchers could consider.

11. Open issues, challenges, and recommendations

Table 10 shows that researchers are gaining interests in the use of blockchain and SDN/NFV in the area of IoT security, including the smart-home security. Smart-home security, as well as the development and vulgarization of smart-home technologies, are still at the beginning of a new era of modernity. The current trends of security systems based on blockchain, SDN/NFV or both present many advantages as described in the previous sections. However, there are still many limitations. This section presents the open issues and challenges in the security of smart homes.

11.1. Blockchain

Section 5 showed that blockchain could improve smart-home security, especially by reinforcing trust, identity management, decentralization, and access management systems [191]. However, researchers have to fix some remaining issues.

Consensus protocol to match with smart-homes constraints: Applying the current consensus protocols in smart homes could be challenging due to resource-constrained (e.g., low latency, energy cost, communication complexity, and computation costs) IoT devices [70]. To cope with that, in [5,93,95], the authors do not use any consensus protocol in their works. The miner plays that role in addition to its core functions. In other words, the proposed-architectures are centralized on the miner, whereas blockchain promotes decentralization for more robustness. Thus, there is a need to develop a lightweight consensus protocol that matches these constraints and provides more convenience, security, and efficiency [192].

Accuracy: This metric is crucial to evaluate attack detection systems. In [96], the authors propose a system that improves the storage capacity of data and detects ongoing attacks. However, they do not evaluate the proposed architecture regarding the attack detection accuracy. Therefore, the detection performance is unknown and not reliable.

Identity management issues: In smart homes, the identity management of users is crucial for security matters. In [100,106], the homeowner plays an essential role in the proposed architecture based on blockchain and smart contracts for smart-home security. In case an attacker manages to doctor the homeowner's identity, many security issues, including data security and users' privacy, could arise. Therefore, another challenge is to ensure that the legitimate user (homeowner) identity must not be compromised.

Deal with overheads: Another challenge consists of dealing with overheads. Blockchain often leads to overheads such as power outages, network failures, false alerts [95]. These might impact the smart-home security

Intrinsic problem related to blockchain: There are several inherent challenges with blockchain, in particular, scalability, privacy leakage, and selfish mining, that should be solved first before any implementation in smart homes to guarantee a safe and secure home environment [69].

11.2. SDN

As we already discussed, we can take advantage of SDN to improve the security of smart homes. However, as seen in [193], intrinsic properties of SDN could imperil systems to various cyber-threats (e.g., intrusion attacks, spoofing attacks, DoS and DDoS attacks). This could undoubtedly impact the security and performance of the home networks as well. Therefore, we should consider SDN security issues before its implementation in the smart-home environment. For example, in [194], the authors show the potential threats of MITM attacks on SDN and OpenFlow channels in the IoT-Fog scenario.

Moreover, as we already described, the potential of SDN is more significant when coupled with the virtualization technology, NFV. SDN/NFV could represent the near future of network technologies. Nevertheless, in the meanwhile, there are some challenges to overcome, such as reducing security issues. These security issues could be related to the policy-based IoT network security, orchestration over various IoT domains, the inherent security issues of SDN and NFV systems, optimal selection, and deployment of SDN/NFV-based security mechanisms, and security granularity in network slicing [21]. Furthermore, there is a crucial need to analyze the correctness of the SDN programs using formal methods [195–197].

Table 10
Contribution of current studies to IoT and smart-home security regarding BLOCKCHAIN, SDN, and NFV technologies.

	Fundamental advantages	IoT security	Smart-home security
Blockchain-based solutions	Access control; Anonymity; Authentication; Authorization; Availability; Identification; Integrity; Privacy; Robustness; Scalability; Security; Trust	[10,20,83–87,89–91,138,139]	[5,11,93,95,96,100,106,137,140]
SDN-based solutions	Authentication; Availability; Centralized security control; Confidentiality; Flexibility; Network programmability; Obfuscation; Privacy; Scalability; Security; Traffic isolation	[10,21,108,115,138,139]	[6,9,11,108,122,123,126,137,140–142,144]
NFV-based solutions	Flexibility; High availability; Cost reduction; Scalability; Security; Trustworthiness; VNF for security systems	[21,130,131]	[7,9,11,133,141,142,144]

11.3. NFV

NFV is a promising technology for improving the smart-home network and its security. However, this technology still faces open issues and challenges [198]. These challenges should be tackled to avoid any downsides in the security of smart homes.

Function virtualization: The main challenge is related to virtualized functions, which should ensure high performance of the system, support multi-tenancy, and be OS-independent.

Portability: VNFs should fit in multi-vendor environments. Portability remains a challenge in NFV.

Standard interfaces: The challenge is to develop a flexible and efficient API that could support both northbound and southbound communications.

Function deployment: The authors highlight the importance of fine-grained deployment and the control and management of network functions.

Traffic steering: This challenge concerns the combination of SDN and NFV. In a software-defined NFV architecture, it is challenging to achieve online computing. SDN and NFV introduce more variables that complicate the unified optimization problem. Moreover, security issues associated with each layer of NFV could lead to additional challenges.

NFVI layer: On this layer, security issues are related to hypervisor vulnerabilities, shared physical resources, lack of control and monitoring, and inconsistent service composition. Some countermeasures include regular VM updates and patches, network isolation and segmentation, security monitoring and intrusion detection, and defense in depth with well-defined policy enforcement.

VNFs layer: This layer suffers from the lack of interoperability, control and monitoring, and insecure interfaces. Improving network security through encryption, access control, and policy enforcement could reinforce the security of this layer.

NFV MANO layer: Many critical threats relate to this layer, including management and control plane attacks, inconsistency in orchestration and management module, and lack of clearly defined policy. Some recommendations include solutions-based for ensuring controller availability, transparency to network control and management, and guaranteeing the security management, orchestration, and automation for improving the end-user experience. Furthermore, as shown in [199], NFV faces isolation failure risks—for instance, denial of service protection failures between hypervisors and VNFs, regulatory compliance failures, infrastructure logs leaking, and internal security risks due to humans (unintended or intended) factor.

11.4. Other challenges

In addition to the previous challenges, we can mention four additional challenges, including identity management of devices, risks assessment methods, information flow approaches, and security management methods [200]. Furthermore, special attention should be given to the security of IoT devices such as VCS that represent a centerpiece in the management of the smart home. Moreover, this area needs comprehensive studies regarding metrics that could provide a precise evaluation of smart-home security. An ongoing challenge consists of developing an evaluation strategy regarding performance and security aspects of smart-home architectures. Finally, there is the human factor that represents a big issue in the security of smart homes. According to IBM [201], over 95% of security breaches are caused by human error. In the case of smart homes, users do not have technical IT skills and knowledge to manage securely and appropriately IoT technologies. Thus, the human factor is a critical problem to solve.

11.5. Recommendations

- Our primary recommendation relates to the existing vulnerabilities and attacks on smart homes described in this paper. We highly recommend future work investigating the hardware, firmware, and software security of everyday IoT devices used in smart homes. Furthermore, voice assistants and smart speakers are essential to the success of smart homes. Therefore, we encourage thorough research to mitigate cyberattacks using inaudible voice commands.

- This survey paper investigates the contribution of blockchain, SDN, and NFV to reinforcing the smart-home security. The challenges described above showed that each of these technologies needs improvement. Therefore, we encourage researchers to fix the challenges aforementioned when building smart-home security solutions to avoid additional attack surfaces.
- We have proposed a hybrid security solution consisting of blockchain, SDN, and NFV to reinforce the smart-home security. Future work could simulate and evaluate the performances of this proposed architecture to appreciate its effectiveness.
- In addition, we encourage interested researchers in smart-home security to investigate fog and edge technologies to overcome the limitations of centralized cloud servers. In a recent survey [202], Rahimi, Songhorabadi, and Kashani showed that building fog computing architecture in smart homes could solve multiple issues facing traditional architectures. Furthermore, implementing a hybrid architecture composed of fog computing, SDN, and blockchain could enhance the smart-home security. Sharma, Chen, and Park [203] have proposed an architecture using these technologies to ensure the security, resiliency, low latency, high availability, real-time data delivery, and high scalability of IoT services.
- Moreover, security is not only a matter of technology. The human factor is also critical. IT security education and promotion of awareness on best practices for securing a smart-home environment should be a top priority. Users, such as children, adults, and the elderly, should have the necessary information on cybersecurity to make the right decisions regarding their safety and security in smart homes.

12. Conclusions

The smart home is one promising application of the Internet of Things promoting remote control over IoT devices to make everyday life at home more convenient. This paper reviewed the literature on smart homes from a security perspective. The goal was to highlight the significant contributions of distinctly blockchain, SDN, and NFV for the smart-home security. We proposed an architecture to secure smart homes using a hybrid security solution. First, we thoroughly described how the smart-home technology works. Then, we pointed out security issues in smart homes related to many aspects such as IoT devices, home networks, applications, cloud technologies, and home users. As solutions to these problems, we have highlighted the benefits of blockchain, SDN and NFV in improving the security of smart homes. Taking full advantage of these security solutions would require fixing existing security issues regarding each of these technologies. Future work could consider implementing and evaluating other technologies such as edge and fog computing when designing a more robust and secure smart home. Furthermore, the challenges regarding smart-home security are not only regarding using the most appropriate technologies. The human factor is also an essential factor in the security chain. Investigating the cybersecurity awareness and behaviors of smart-home users is another future direction to explore. Even though we are still at the beginning of the smart-home technology, this survey provides an overview of the current trends, vulnerabilities, technology-aware security solutions, listed open issues and challenges, and recommendations for the smart-home security. Moreover, the survey guides academic researchers and industry professionals through various insights and research directions.

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

The authors would like to thank the anonymous reviewers for their comprehensive review of this paper. This work was funded by the Japanese Government (Monbukagakusho: MEXT) scholarship. Moreover, this work was partially supported by the Wallenberg AI, Autonomous Systems and Software Program (WASP) funded by Knut and Alice Wallenberg Foundation.

References

[1] B. Reeder, A. David, Health at hand: a systematic review of smart watch uses for health and wellness, J. Biomed. Inform. 63 (2016) 269–276.
[2] L. Jiang, D.-Y. Liu, B. Yang, Smart home research, in: Proceedings of 2004 International Conference on Machine Learning and Cybernetics (IEEE Cat. No. 04EX826), Vol. 2, IEEE, 2004, pp. 659–663.
[3] Statista, Smart Home Report 2021, 2021, [Online; accessed: June 30, 2022]. URL https://www.statista.com/study/42112/smart-home-report/.
[4] SonicWall, 2022 SonicWall Cyber Threat Report, sonicwall, 2022, [Online; accessed: June 16, 2022]. URL https://www.sonicwall.com/2022-cyber-threat-report/.
[5] A. Dorri, S.S. Kanhere, R. Jurdak, P. Gauravaram, Blockchain for IoT security and privacy: The case study of a smart home, in: 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), IEEE, 2017, pp. 618–623.
[6] P.K. Sharma, J.H. Park, Y.-S. Jeong, J.H. Park, SHSec: SDN based secure smart home network architecture for internet of things, Mob. Netw. Appl. 24 (3) (2019) 913–924.
[7] Y. Afek, A. Bremler-Barr, D. Hay, R. Goldschmidt, L. Shafir, G. Avraham, A. Shalev, NFV-based IoT security for home networks using MUD, in: NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium, IEEE, 2020, pp. 1–9.
[8] Web of Science, Discover multidisciplinary content from the world's most trusted global citation database, 2022, [Online; accessed: June 16, 2022]. URL https://www.webofscience.com/wos/woscc/basic-search.
[9] S. Luo, J. Wu, J. Li, L. Guo, A multi-stage attack mitigation mechanism for software-defined home networks, IEEE Trans. Consum. Electron. 62 (2) (2016) 200–207.
[10] S.A. Latif, F.B.X. Wen, C. Iwendi, L. li F. Wang, S.M. Mohsin, Z. Han, S.S. Band, AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems, Comput. Commun. 181 (2022) 274–283, http://dx.doi.org/10.1016/j.comcom.2021.09.029.

[11] A. Rahman, M.J. Islam, F.A. Sunny, M.K. Nasir, DistBlockSDN: A distributed secure blockchain based SDN-IoT architecture with NFV implementation for smart cities, in: 2019 2nd International Conference on Innovation in Engineering and Technology (ICIET), 2019, pp. 1–6, http://dx.doi.org/10.1109/ICIET48527.2019.9290627.

[12] D. Bastos, M. Shackleton, F. El-Moussa, Internet of things: A survey of technologies and security risks in smart home and city environments, in: Living in the Internet of Things: Cybersecurity of the IoT - 2018, IET, 2018, pp. 1–7.

[13] M. Khawla, M. Tomader, A survey on the security of smart homes: Issues and solutions, in: Proceedings of the 2nd International Conference on Smart Digital Environment, ACM, 2018, pp. 81–87.

[14] D. Mocrii, Y. Chen, P. Musilek, IoT-based smart homes: A review of system architecture, software, communications, privacy and security, Internet Things 1 (2018) 81–98.

[15] J.J. Barriga A, S.G. Yoo, Security over smart home automation systems: A survey, in: International Conference of Research Applied to Defense and Security, Springer, 2018, pp. 87–96.

[16] M.K. Kuyucu, Ş. Bahtiyar, G. İnce, Security and privacy in the smart home: A survey of issues and mitigation strategies, in: 2019 4th International Conference on Computer Science and Engineering (UBMK), 2019, pp. 113–118, http://dx.doi.org/10.1109/UBMK.2019.8907037.

[17] N. Panwar, S. Sharma, S. Mehrotra, L. Krzywiecki, N. Venkatasubramanian, Smart home survey on security and privacy, 2019, CoRR abs/1904.05476. arXiv:1904.05476.

[18] Q.I. Sarhan, Systematic survey on smart home safety and security systems using the arduino platform, IEEE Access 8 (2020) 128362–128384, http://dx.doi.org/10.1109/ACCESS.2020.3008610.

[19] S. AlJanah, N. Zhang, S.W. Tay, A survey on smart home authentication: Toward secure, multi-level and interaction-based identification, IEEE Access 9 (2021) 130914–130927, http://dx.doi.org/10.1109/ACCESS.2021.3114152.

[20] M.A. Khan, K. Salah, IoT security: Review, blockchain solutions, and open challenges, Future Gener. Comput. Syst. 82 (2018) 395–411.

[21] I. Farris, T. Taleb, Y. Khettab, J. Song, A survey on emerging SDN and NFV security mechanisms for IoT systems, IEEE Commun. Surv. Tutor. 21 (1) (2018) 812–837.

[22] T. Mendes, R. Godina, E. Rodrigues, J. Matias, J. Catalão, Smart home communication technologies and applications: Wireless protocol assessment for home area network resources, Energies 8 (7) (2015) 7279–7311, http://dx.doi.org/10.3390/en8077279.

[23] H.A. Gabbar, Building energy management systems (BEMS), in: Energy Conservation in Residential, Commercial, and Industrial Facilities, Wiley-IEEE Press, 2018, pp. 15–81.

[24] UN, World Population Ageing 2017 - Highlights, 2017.

[25] Q. Lê, H.B. Nguyen, T. Barnett, Smart homes for older people: Positive aging in a digital world, Future Internet 4 (2) (2012) 607–617.

[26] K. Matthews, The internet of robotic things: How IoT and robotics tech are evolving together, 2019, [Online; accessed: June 16, 2022]. URL https://iot.eetimes.com/the-internet-of-robotic-things-how-iot-and-robotics-tech-are-evolving-together/.

[27] G. Wilson, C. Pereyda, N. Raghunath, G. de la Cruz, S. Goel, S. Nesaei, B. Minor, M. Schmitter-Edgecombe, M.E. Taylor, D.J. Cook, Robot-enabled support of daily activities in smart home environments, Cogn. Syst. Res. 54 (2019) 258–272.

[28] B.L.R. Stojkoska, K.V. Trivodaliev, A review of Internet of Things for smart home: Challenges and solutions, J. Cleaner Prod. 140 (2017) 1454–1464.

[29] M.R. Alam, M.B.I. Reaz, M.A.M. Ali, A review of smart homes - Past, present, and future, IEEE Trans. Syst. Man Cybern. C 42 (6) (2012) 1190–1203.

[30] T. Denning, T. Kohno, H.M. Levy, Computer security and the modern home, Commun. ACM 56 (1) (2013) 94–103, http://dx.doi.org/10.1145/2398356.2398377.

[31] Y. Yang, L. Wu, G. Yin, L. Li, H. Zhao, A survey on security and privacy issues in Internet-of-Things, IEEE Internet Things J. 4 (5) (2017) 1250–1258.

[32] A. Hameed, A. Alomary, Security issues in IoT: A survey, in: 2019 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), 2019, pp. 1–5, http://dx.doi.org/10.1109/3ICT.2019.8910320.

[33] T. Edmund Brumaghin, Vulnerability spotlight: Multiple vulnerabilities in Samsung SmartThings Hub, 2018, [Online; accessed: June 16, 2022]. URL https://blog.talosintelligence.com/2018/07/samsung-smartthings-vulns.html?m=1.

[34] E. Fernandes, J. Jung, A. Prakash, Security analysis of emerging smart home applications, in: 2016 IEEE Symposium on Security and Privacy (SP), 2016, pp. 636–654, http://dx.doi.org/10.1109/SP.2016.44.

[35] K. Tian, Your home was not so secure after all, 2017, [Online; accessed: June 16, 2022]. URL https://medium.com/hackernoon/your-home-was-not-so-secure-after-all-af52fbd6777c.

[36] Z. Hall, Zero-day iOS HomeKit vulnerability allowed remote access to smart accessories including locks, fix rolling out, 2017, [Online; accessed: June 16, 2022]. URL https://9to5mac.com/2017/12/07/homekit-vulnerability/.

[37] V. Sivaraman, H.H. Gharakheili, A. Vishwanath, R. Boreli, O. Mehani, Network-level security and privacy control for smart-home IoT devices, in: 2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE, 2015, pp. 163–167.

[38] E. Metalidou, C. Marinagi, P. Trivellas, N. Eberhagen, C. Skourlas, G. Giannakopoulos, The human factor of information security: Unintentional damage perspective, Procedia-Soc. Behav. Sci. 147 (2014) 424–428.

[39] S. Kraemer, P. Carayon, J. Clem, Human and organizational factors in computer and information security: Pathways to vulnerabilities, Comput. Secur. 28 (7) (2009) 509–520.

[40] OWASP, OWASP internet of things project, 2019, [Online; accessed: June 16, 2022]. URL https://owasp.org/www-project-internet-of-things/.

[41] S. Kottler, February 28th ddos incident report, 2018, [Online; accessed: June 16, 2022]. URL https://github.blog/2018-03-01-ddos-incident-report/.

[42] KrebsonSecurity, DDoS on dyn impacts Twitter, spotify, reddit, 2016, [Online; accessed: June 16, 2022]. URL https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/.

[43] O. Olawumi, K. Haataja, M. Asikainen, N. Vidgren, P. Toivanen, Three practical attacks against ZigBee security: Attack scenario definitions, practical experiments, countermeasures, and lessons learned, in: 2014 14th International Conference on Hybrid Intelligent Systems, IEEE, 2014, pp. 199–206.

[44] J.J. Kang, K. Fahd, S. Venkatraman, R. Trujillo-Rasua, P. Haskell-Dowland, Hybrid routing for man-in-the-middle (MITM) attack detection in IoT networks, in: 2019 29th International Telecommunication Networks and Applications Conference (ITNAC), 2019, pp. 1–6, http://dx.doi.org/10.1109/ITNAC46935.2019.9077977.

[45] N. Apthorpe, D. Reisman, S. Sundaresan, A. Narayanan, N. Feamster, Spying on the smart home: Privacy attacks and defenses on encrypted IoT traffic, 2017, CoRR abs/1708.05044. arXiv:1708.05044. URL http://arxiv.org/abs/1708.05044.

[46] Z. Feng, J. Ning, I. Broustis, K. Pelechrinis, S.V. Krishnamurthy, M. Faloutsos, Coping with packet replay attacks in wireless networks, in: 2011 8th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, IEEE, 2011, pp. 368–376.

[47] G. He, Requirements for security in home environments, in: Residential and Virtual Home Environments Seminar on Internetworking, Spring, 2002.

[48] A. Hamed, A.A. Khalek, Acoustic attacks in the era of IoT-A survey, in: 2019 Amity International Conference on Artificial Intelligence (AICAI), IEEE, 2019, pp. 855–858.

[49] Y. Gong, C. Poellabauer, An overview of vulnerabilities of voice controlled systems, 2018, CoRR abs/1803.09156. arXiv:1803.09156.

[50] X. Yuan, P. He, Q. Zhu, X. Li, Adversarial examples: Attacks and defenses for deep learning, IEEE Trans. Neural Netw. Learn. Syst. (2019).

[51] N. Zhang, X. Mi, X. Feng, X. Wang, Y. Tian, F. Qian, Dangerous skills: Understanding and mitigating security risks of voice-controlled third-party functions on virtual personal assistant systems, in: 2019 IEEE Symposium on Security and Privacy (SP), 2019, pp. 1381–1396, http://dx.doi.org/10.1109/SP.2019.00016.

[52] D. Kumar, R. Paccagnella, P. Murley, E. Hennenfent, J. Mason, A. Bates, M. Bailey, Skill squatting attacks on amazon alexa, in: 27th USENIX Security Symposium (USENIX Security 18), 2018, pp. 33–47.

[53] T. Sugawara, B. Cyr, S. Rampazzi, D. Genkin, K. Fu, Light commands: Laser-based audio injection on voice-controllable systems, 2019.

[54] S.N. Patel, M.S. Reynolds, G.D. Abowd, Detecting human movement by differential air pressure sensing in HVAC system ductwork: An exploration in infrastructure mediated sensing, in: International Conference on Pervasive Computing, Springer, 2008, pp. 1–18.

[55] M. Chin, Millions of baby monitors, security cameras easy to hack, 2018, [Online; accessed: June 16, 2022]. URL https://www.tomsguide.com/us/cheap-security-cameras-poor-passwords,news-27495.html.

[56] A.B. Wang, 'I'm in your baby's room': A hacker took over a baby monitor and broadcast threats, parents say, 2018, [Online; accessed: June 16, 2022]. URL https://www.washingtonpost.com/technology/2018/12/20/nest-cam-baby-monitor-hacked-kidnap-threat-came-device-parents-say/?noredirect=on.

[57] F.-X. Standaert, Introduction to side-channel attacks, in: Secure Integrated Circuits and Systems, Springer, 2010, pp. 27–42.

[58] M.A.N. Abrishamchi, A.H. Abdullah, A.D. Cheok, K.S. Bielawski, Side channel attacks on smart home systems: A short overview, in: IECON 2017-43rd Annual Conference of the IEEE Industrial Electronics Society, IEEE, 2017, pp. 8144–8149.

[59] G. Deepa, G. SriTeja, S. Venkateswarlu, An overview of acoustic side-channel attack, Int. J. Comput. Sci. Commun. Netw. 3 (1) (2013) 15–20.

[60] A. Sayakkara, N.-A. Le-Khac, M. Scanlon, Leveraging electromagnetic side-channel analysis for the investigation of IoT devices, Digit. Investig. 29 (S) (2019) S94–S103, http://dx.doi.org/10.1016/j.diin.2019.04.012.

[61] V. Srinivasan, J. Stankovic, K. Whitehouse, Protecting your daily in-home activity information from a wireless snooping attack, in: Proceedings of the 10th International Conference on Ubiquitous Computing, ACM, 2008, pp. 202–211.

[62] A. Pope, Essay on Criticism, CUP Archive, 1728.

[63] D.U. Case, Analysis of the Cyber Attack on the Ukrainian Power Grid, Electricity Information Sharing and Analysis Center (E-ISAC), 2016.

[64] D. Gan, R. Heartfield, Social engineering in the internet of everything, Cutter IT J. 29 (7) (2016) 20–29.

[65] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno, et al., Comprehensive experimental analyses of automotive attack surfaces, in: USENIX Security Symposium, Vol. 4, San Francisco, 2011, pp. 447–462.

[66] V. Sivaraman, D. Chan, D. Earl, R. Boreli, Smart-phones attacking smart-homes, in: Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks, ACM, 2016, pp. 195–200.

[67] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2008, URL https://bitcoin.org/bitcoin.pdf.

[68] M. Swan, Blockchain: Blueprint for a New Economy, " O'Reilly Media, Inc.", 2015.

[69] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, H. Wang, Blockchain challenges and opportunities: A survey, Int. J. Web Grid Serv. 14 (2018) 352, http://dx.doi.org/10.1504/IJWGS.2018.095647.

[70] I. Makhdoom, M. Abolhasan, H. Abbas, W. Ni, Blockchain's adoption in IoT: The challenges, and a way forward, J. Netw. Comput. Appl. (2018).

[71] I.-C. Lin, T.-C. Liao, A survey of blockchain security issues and challenges, IJ Netw. Secur. 19 (5) (2017) 653–659.

[72] M. Salimitari, M. Chatterjee, An overview of blockchain and consensus protocols for IoT networks, 2018, ArXiv abs/1809.05613.

[73] N. Szabo, Smart contracts : Building blocks for digital markets, EXTROPY: J. Transhumanist Thought 18 (16) (1996).

[74] ONF, Software-defined networking (SDN) definition, 2019, [Online; accessed: June 16, 2022]. URL https://www.opennetworking.org/sdn-definition/.

[75] D. Kreutz, F. Ramos, P. Verissimo, C.E. Rothenberg, S. Azodolmolky, S. Uhlig, Software-defined networking: A comprehensive survey, 2014, arXiv preprint arXiv:1406.0440.

[76] N. Feamster, J. Rexford, E. Zegura, The road to SDN: an intellectual history of programmable networks, ACM SIGCOMM Comput. Commun. Rev. 44 (2) (2014) 87–98.

[77] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, J. Turner, OpenFlow: enabling innovation in campus networks, ACM SIGCOMM Comput. Commun. Rev. 38 (2) (2008) 69–74.

[78] E. Haleplidis, S. Denazis, K. Pentikousis, J.H. Salim, D. Meyer, O. Koufopavlou, SDN Layers and Architecture Terminology, Internet Draft, Internet Engineering Task Force, 2014.

[79] P. Tijare, D. Vasudevan, The northbound APIs of software defined networks, Int. J. Eng. Sci. Res. Technol. (2016).

[80] H. Hawilo, A. Shami, M. Mirahmadi, R. Asal, NFV: State of the art, challenges and implementation in next generation mobile networks (vEPC), 2014, arXiv preprint arXiv:1409.4149.

[81] ETSI, Network Functions Virtualisation (NFV); Virtual Network Functions Architecture, ETSI, 2014, [Online; accessed: June 16, 2022]. URL https://www.etsi.org/deliver/etsi_gs/NFV-SWA/001_099/001/01.01.01_60/gs_NFV-SWA001v010101p.pdf.

[82] ETSI, Network Functions Virtualisation (NFV); Management and Orchestration, ETSI, 2014, [Online; accessed: June 16, 2022]. URL https://www.etsi.org/deliver/etsi_gs/NFV-MAN/001_099/001/01.01.01_60/gs_NFV-MAN001v010101p.pdf.

[83] N.Z. Aitzhan, D. Svetinovic, Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams, IEEE Trans. Dependable Secure Comput. 15 (5) (2018) 840–852, http://dx.doi.org/10.1109/TDSC.2016.2616861.

[84] K. Biswas, V. Muthukkumarasamy, Securing smart cities using blockchain technology, in: 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 2016, pp. 1392–1393, http://dx.doi.org/10.1109/HPCC-SmartCity-DSS.2016.0198.

[85] P.K. Sharma, J.H. Park, Blockchain based hybrid network architecture for the smart city, Future Gener. Comput. Syst. 86 (2018) 650–655, http://dx.doi.org/10.1016/j.future.2018.04.060, URL https://www.sciencedirect.com/science/article/pii/S0167739X1830431X.

[86] K. Christidis, M. Devetsikiotis, Blockchains and smart contracts for the internet of things, IEEE Access 4 (2016) 2292–2303, http://dx.doi.org/10.1109/ACCESS.2016.2566339.

[87] N. Kshetri, Blockchain's roles in strengthening cybersecurity and protecting privacy, Telecommun. Policy 41 (10) (2017) 1027–1038.

[88] W. Xie, Y. Jiang, Y. Tang, N. Ding, Y. Gao, Vulnerability detection in IoT firmware: A survey, in: 2017 IEEE 23rd International Conference on Parallel and Distributed Systems (ICPADS), 2017, pp. 769–772, http://dx.doi.org/10.1109/ICPADS.2017.00104.

[89] B. Lee, J.-H. Lee, Blockchain-based secure firmware update for embedded devices in an Internet of Things environment, J. Supercomput. 73 (3) (2017) 1152–1167.

[90] M.S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, M.H. Rehmani, Applications of blockchains in the internet of things: A comprehensive survey, IEEE Commun. Surv. Tutor. (2018).

[91] D. Minoli, B. Occhiogrosso, Blockchain mechanisms for IoT security, Internet Things 1 (2018) 1–13.

[92] F. Osterlind, A. Dunkels, J. Eriksson, N. Finne, T. Voigt, Cross-level sensor network simulation with cooja, in: Proceedings. 2006 31st IEEE Conference on Local Computer Networks, IEEE, 2006, pp. 641–648.

[93] A. Dorri, S.S. Kanhere, R. Jurdak, Towards an optimized blockchain for IoT, in: Proceedings of the Second International Conference on Internet-of-Things Design and Implementation, ACM, 2017, pp. 173–178.

[94] ns-3, Network simulator, 2020, [Online; accessed: June 23, 2022]. URL https://www.nsnam.org.

[95] S. Sudhakar, Blockchain enabled smart home community system, Ijtet 36 (2019).

[96] C. Qu, M. Tao, R. Yuan, A hypergraph-based blockchain model and application in internet of things-enabled smart homes, Sensors 18 (9) (2018) 2784.

[97] W. She, Z.-H. Gu, X.-K. Lyu, Q. Liu, Z. Tian, W. Liu, Homomorphic consortium blockchain for smart home system sensitive data privacy preserving, IEEE Access 7 (2019) 62058–62070, http://dx.doi.org/10.1109/ACCESS.2019.2916345.

[98] S. Arif, M.A. Khan, S.U. Rehman, M.A. Kabir, M. Imran, Investigating smart home security: Is blockchain the answer? IEEE Access 8 (2020) 117802–117816, http://dx.doi.org/10.1109/ACCESS.2020.3004662.

[99] S. Singh, I.-H. Ra, W. Meng, M. Kaur, G.H. Cho, 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) (2019) 1550147719844159, http://dx.doi.org/10.1177/1550147719844159, arXiv:https://doi.org/10.1177/1550147719844159.

[100] T.L.N. Dang, M.S. Nguyen, An approach to data privacy in smart home using blockchain technology, in: 2018 International Conference on Advanced Computing and Applications (ACOMP), 2018, pp. 58–64, http://dx.doi.org/10.1109/ACOMP.2018.00017.

[101] Truffle, Ganache, 2022, [Online; accessed: June 30, 2022]. URL https://www.trufflesuite.com/ganache.

[102] Remix, Home, 2021, [Online; accessed: June 30, 2022]. URL https://remix.ethereum.org.

[103] Ethereum, JavaScript API, 2020, [Online; accessed: June 30, 2022]. URL https://github.com/ethereum/wiki/wiki/JavaScript-API.

[104] K.M. Giannoutakis, G. Spathoulas, C.K. Filelis-Papadopoulos, A. Collen, M. Anagnostopoulos, K. Votis, N.A. Nijdam, A blockchain solution for enhancing cybersecurity defence of IoT, in: 2020 IEEE International Conference on Blockchain (Blockchain), 2020, pp. 490–495, http://dx.doi.org/10.1109/Blockchain50366.2020.00071.

[105] A. Qashlan, P. Nanda, X. He, M. Mohanty, Privacy-preserving mechanism in smart home using blockchain, IEEE Access 9 (2021) 103651–103669, http://dx.doi.org/10.1109/ACCESS.2021.3098795.

[106] Y. Zhou, M. Han, L. Liu, Y. Wang, Y. Liang, L. Tian, 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, 2018, pp. 81–87.

[107] R. Sherwood, G. Gibb, K.-K. Yap, G. Appenzeller, M. Casado, N. McKeown, G. Parulkar, Flowvisor: A network virtualization layer, in: OpenFlow Switch Consortium, Tech. Rep 1, 2009, p. 132.

[108] M. Boussard, D.T. Bui, L. Ciavaglia, R. Douville, M. Le Pallec, N. Le Sauze, L. Noirie, S. Papillon, P. Peloso, F. Santoro, Software-defined LANs for interconnected smart environment, in: 2015 27th International Teletraffic Congress, IEEE, 2015, pp. 219–227.

[109] R. Braga, E. de Souza Mota, A. Passito, Lightweight DDoS flooding attack detection using NOX/OpenFlow, in: LCN, Vol. 10, 2010, pp. 408–415.

[110] Q. Yan, F.R. Yu, Q. Gong, J. Li, Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges, IEEE Commun. Surv. Tutor. 18 (1) (2015) 602–622.

[111] S.W. Shin, G. Gu, Cloudwatcher: Network security monitoring using openflow in dynamic cloud networks, in: Network Protocols (ICNP) 2012, IEEE, 2012, pp. 1–6.

[112] S.A. Mehdi, J. Khalid, S.A. Khayam, Revisiting traffic anomaly detection using software defined networking, in: International Workshop on Recent Advances in Intrusion Detection, Springer, 2011, pp. 161–180.

[113] N.Z. Bawany, J.A. Shamsi, K. Salah, DDoS attack detection and mitigation using SDN: methods, practices, and solutions, Arab. J. Sci. Eng. 42 (2) (2017) 425–441.

[114] C. Yoon, T. Park, S. Lee, H. Kang, S. Shin, Z. Zhang, Enabling security functions with SDN: A feasibility study, Comput. Netw. 85 (2015) 19–35.

[115] S. Chakrabarty, D.W. Engels, S. Thathapudi, Black SDN for the internet of things, in: 2015 IEEE 12th International Conference on Mobile Ad Hoc and Sensor Systems, IEEE, 2015, pp. 190–198.

[116] S.W. Shin, P. Porras, V. Yegneswara, M. Fong, G. Gu, M. Tyson, FRESCO: Modular composable security services for software-defined networks, in: 20th Annual Network & Distributed System Security Symposium, Ndss, 2013.

[117] J. Sonchack, J.M. Smith, A.J. Aviv, E. Keller, Enabling practical software-defined networking security applications with OFX, in: NDSS, Vol. 16, 2016, pp. 1–15.

[118] W. Iqbal, H. Abbas, P. Deng, J. Wan, B. Rauf, Y. Abbas, I. Rashid, ALAM: Anonymous lightweight authentication mechanism for SDN-enabled smart homes, IEEE Internet Things J. 8 (12) (2021) 9622–9633, http://dx.doi.org/10.1109/JIOT.2020.3024058.

[119] W. Iqbal, H. Abbas, B. Rauf, Y. Abbas, F. Amjad, A. Hemani, PCSS: Privacy preserving communication scheme for SDN enabled smart homes, IEEE Sens. J. (2021) 1, http://dx.doi.org/10.1109/JSEN.2021.3087779.

[120] S. Wang, K.M. Gomez, K. Sithamparanathan, P. Zanna, Software defined network security framework for IoT based smart home and city applications, in: 2019 13th International Conference on Signal Processing and Communication Systems (ICSPCS), 2019, pp. 1–8, http://dx.doi.org/10.1109/ICSPCS47537.2019.9008703.

[121] M.H. Bhuyan, D.K. Bhattacharyya, J.K. Kalita, Surveying port scans and their detection methodologies, Comput. J. 54 (10) (2011) 1565–1581.

[122] S. Shirali-Shahreza, Y. Ganjali, Protecting home user devices with an SDN-based firewall, IEEE Trans. Consum. Electron. 64 (1) (2018) 92–100.

[123] M. Ge, J.B. Hong, S.E. Yusuf, D.S. Kim, Proactive defense mechanisms for the software-defined internet of things with non-patchable vulnerabilities, Future Gener. Comput. Syst. 78 (2018) 568–582.

[124] iPerf, iPerf - The ultimate speed test tool for TCP, UDP and SCTP, 2020, [Online; accessed: June 30, 2022]. URL https://iperf.fr.

[125] S. Shirali-Shahreza, FleXight: Flexible Information Channel for Software-Defined Networking (Ph.D. thesis), University of Toronto (Canada), 2018.

[126] M. Nobakht, V. Sivaraman, R. Boreli, A host-based intrusion detection and mitigation framework for smart home IoT using OpenFlow, in: 2016 11th International Conference on Availability, Reliability and Security (ARES), IEEE, 2016, pp. 147–156.

[127] H. Gordon, C. Park, B. Tushir, Y. Liu, B. Dezfouli, An efficient SDN architecture for smart home security accelerated by FPGA, in: 2021 IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN), 2021, pp. 1–3, http://dx.doi.org/10.1109/LANMAN52105.2021.9478836.

[128] H. Gordon, C. Batula, B. Tushir, B. Dezfouli, Y. Liu, Securing smart homes via software-defined networking and low-cost traffic classification, in: 2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC), 2021, pp. 1049–1057, http://dx.doi.org/10.1109/COMPSAC51774.2021.00143.

[129] J. Bhayo, S. Hameed, S.A. Shah, An efficient counter-based ddos attack detection framework leveraging software defined IoT (SD-IoT), IEEE Access 8 (2020) 221612–221631, http://dx.doi.org/10.1109/ACCESS.2020.3043082.

[130] H. Oh, S. Ahn, J. Yang, J.K. Choi, A study on trustworthy cyber-physical ID/Location mapping on IoT and NFV, Softw. Netw. 2018 (1) (2018) 1–18.

[131] H. Yang, Y. Kim, Design and implementation of high-availability architecture for IoT-cloud services, Sensors 19 (15) (2019) 3276.

[132] E. Lear, R. Droms, D. Romascanu, RFC 8520: Manufacturer Usage Description Specification, Internet Engineering Task Force, 2019, March.

[133] R. Sairam, S.S. Bhunia, V. Thangavelu, M. Gurusamy, NETRA: Enhancing IoT security using NFV-based edge traffic analysis, IEEE Sens. J. 19 (12) (2019) 4660–4671.

[134] GenieACS, Fast, lightweight TR-069 ACS, 2019, [Online; accessed: June 30, 2022]. URL https://genieacs.com/.

[135] Docker, Debug your app, not your environment, 2020, [Online; accessed: June 30, 2022]. URL https://www.docker.com.

[136] sepehrdaddev, Xerxes dos tool enhanced, 2018, [Online; accessed: June 30, 2022]. URL https://github.com/sepehrdaddev/Xerxes.

[137] M. Boussard, S. Papillon, P. Peloso, M. Signorini, E. Waisbard, STewARD: SDN and blockchain-based trust evaluation for automated risk management on IoT devices, in: IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), IEEE, 2019, pp. 841–846.

[138] P.K. Sharma, S. Singh, Y.-S. Jeong, J.H. Park, DistBlockNet: A distributed blockchains-based secure SDN architecture for IoT networks, IEEE Commun. Mag. 55 (9) (2017) 78–85, http://dx.doi.org/10.1109/MCOM.2017.1700041.

[139] Z. Zeng, X. Zhang, Z. Xia, Intelligent blockchain-based secure routing for multidomain SDN-enabled IoT networks, Wirel. Commun. Mob. Comput. 2022 (2022) http://dx.doi.org/10.1155/2022/5693962.

[140] N. Rajabi, J. Qaddour, SDIoBoT: A software-defined internet of blockchains of things model, Int. J. Internet Things 8 (1) (2019) 17–26.

[141] S. Luo, H. Wang, J. Wu, J. Li, L. Guo, B. Pei, How to defend against sophisticated intrusions in home networks using SDN and NFV, in: 2016 IEEE 83rd Vehicular Technology Conference (VTC Spring), 2016, pp. 1–5, http://dx.doi.org/10.1109/VTCSpring.2016.7504274.

[142] M. Al-Shaboti, I. Welch, A. Chen, M.A. Mahmood, Towards secure smart home IoT: Manufacturer and user network access control framework, in: 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA), 2018, pp. 892–899, http://dx.doi.org/10.1109/AINA.2018.00131.

[143] Anastacia, Advanced networked agents for security and trust assessment in CPS / IOT architectures, 2017, [Online; accessed: June 16, 2022]. URL http://www.anastacia-h2020.eu.

[144] A.M. Zarca, J.B. Bernabe, R. Trapero, D. Rivera, J. Villalobos, A. Skarmeta, S. Bianchi, A. Zafeiropoulos, P. Gouvas, Security management architecture for NFV/SDN-aware IoT systems, IEEE Internet Things J. (2019).

[145] Mininet, An instant virtual network on your laptop (or other PC), 2018, [Online; accessed: June 23, 2022]. URL http://mininet.org.

[146] I.D. Alvarenga, G.A. Rebello, O.C.M. Duarte, Securing configuration management and migration of virtual network functions using blockchain, in: NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium, IEEE, 2018, pp. 1–9.

[147] R.P. Pasupulati, J. Shropshire, Analysis of centralized and decentralized cloud architectures, in: SoutheastCon 2016, IEEE, 2016, pp. 1–7.

[148] D. McNickle, K. Pawlikowski, G. Ewing, AKAROA2: A controller of discrete-event simulation which exploits the distributed computing resources of networks, in: ECMS, 2010, pp. 104–109.

[149] PacketTracerNetwork, Packet Tracer 7.1.1 - IoT devices configuration, 2019, [Online; accessed: June 23, 2022]. URL https://www.packettracernetwork.com/internet-of-things/pt7-iot-devices-configuration.html.

[150] K. Mehdi, M. Lounis, A. Bounceur, T. Kechadi, CupCarbon: A multi-agent and discrete event wireless sensor network design and simulation tool, 2014, http://dx.doi.org/10.4108/icst.simutools.2014.254811.

[151] GNS3, Getting started with GNS3, 2022, [Online; accessed: June 30, 2022]. URL https://www.gns3.com.

[152] H. Gupta, A. Dastjerdi, S. Ghosh, R. Buyya, iFogSim: A toolkit for modeling and simulation of resource management techniques in internet of things, edge and fog computing environments, Softw. - Pract. Exp. 47 (2016) http://dx.doi.org/10.1002/spe.2509.

[153] IoTIFY, A new way to test IoT apps, 2020, [Online; accessed: June 30, 2022]. URL https://docs.iotify.io.

[154] M. Salama, Y. Elkhatib, G. Blair, IoTNetSim: A modelling and simulation platform for end-to-end IoT services and networking, in: Proceedings of the 12th IEEE/ACM International Conference on Utility and Cloud Computing, in: UCC'19, Association for Computing Machinery, New York, NY, USA, 2019, pp. 251–261, http://dx.doi.org/10.1145/3344341.3368820.

[155] X. Zeng, S.K. Garg, P. Strazdins, P.P. Jayaraman, D. Georgakopoulos, R. Ranjan, IOTSim: A simulator for analysing IoT applications, J. Syst. Archit. 72 (2017) 93–107, http://dx.doi.org/10.1016/j.sysarc.2016.06.008, Design Automation for Embedded Ubiquitous Computing Systems. URL https://www.sciencedirect.com/science/article/pii/S1383762116300662.

[156] Gambit Communications, MIMIC IoT simulator - MQTT, CoAP, Modbus, HTTP, HTTPS, REST, 2022, [Online; accessed: June 30, 2022]. URL https://www.gambitcomm.com/site/mimic-simulator.php.

[157] HewlettPackard, Netperf, 2021, [Online; accessed: June 30, 2022]. URL https://github.com/HewlettPackard/netperf.

[158] TETCOS, NetSim academic, 2021, [Online; accessed: June 30, 2022]. URL https://tetcos.com/netsim-acad.html.

[159] G.F. Riley, T.R. Henderson, The ns-3 network simulator, in: K. Wehrle, M. Güneş, J. Gross (Eds.), Modeling and Tools for Network Simulation, Springer Berlin Heidelberg, Berlin, Heidelberg, 2010, pp. 15–34, http://dx.doi.org/10.1007/978-3-642-12331-3_2.

[160] A. Varga, R. Hornig, An overview of the OMNeT++ simulation environment, in: Proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems & Workshops, in: Simutools '08, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), Brussels, BEL, 2008.

[161] OMNeT++, Discrete event simulator, 2022, [Online; accessed: June 23, 2022]. URL https://omnetpp.org.

[162] OPNET, OPNET network simulator, 2020, [Online; accessed: June 23, 2022]. URL http://opnetprojects.com/opnet-network-simulator/.

[163] M. Chen, Y. Miao, I. Humar, OPNET IoT Simulation, Springer Nature, 2019.

[164] S. Sotiriadis, N. Bessis, E. Asimakopoulou, N. Mustafee, Towards simulating the internet of things, in: 2014 28th International Conference on Advanced Information Networking and Applications Workshops, 2014, pp. 444–448, http://dx.doi.org/10.1109/WAINA.2014.74.

[165] B. Musznicki, P. Zwierzykowski, Survey of simulators for wireless sensor networks, Int. J. Grid Distrib. Comput. 5 (3) (2012) 23–50.

[166] N. Alshammari, T. Alshammari, M. Sedky, J. Champion, C. Bauer, Openshs: Open smart home simulator, Sensors 17 (5) (2017) 1003.

[167] Y. Francillette, E. Boucher, A. Bouzouane, S. Gaboury, The virtual environment for rapid prototyping of the intelligent environment, Sensors 17 (11) (2017) http://dx.doi.org/10.3390/s17112562.

[168] B. Ho, D. Vogts, J. Wesson, A smart home simulation tool to support the recognition of activities of daily living, in: Proceedings of the South African Institute of Computer Scientists and Information Technologists 2019, in: SAICSIT '19, Association for Computing Machinery, New York, NY, USA, 2019, http://dx.doi.org/10.1145/3351108.3351132.

[169] Y. Mirsky, A. Shabtai, L. Rokach, B. Shapira, Y. Elovici, Sherlock vs moriarty: A smartphone dataset for cybersecurity research, in: Proceedings of the 2016 ACM Workshop on Artificial Intelligence and Security, 2016, pp. 1–12.

[170] CVE, CVE list home, 2021, [Online; accessed: June 30, 2022]. URL https://cve.mitre.org.

[171] WAND, WITS: ISPDSL-II, 2010, [Online; accessed: June 30, 2022]. URL https://wand.net.nz/wits/ispdsl/2/.

[172] OpenSHS, OpenSHS: Open smart home simulator, 2021, [Online; accessed: June 30, 2022]. URL https://openshs.github.io/openshs/.

[173] Iannyck, SHIMA: Smart home sIMulAtor, 2018, [Online; accessed: June 30, 2022]. URL https://github.com/Iannyck/shima.

[174] M. Timothy, SESim: Smart environment simulator, 2020, [Online; accessed: June 30, 2022]. URL https://github.com/timothymush7/SeSim-1.1.

[175] N. Moustafa, J. Slay, UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set), in: 2015 Military Communications and Information Systems Conference (MilCIS), 2015, pp. 1–6, http://dx.doi.org/10.1109/MilCIS.2015.7348942.

[176] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, A. Shabtai, D. Breitenbacher, Y. Elovici, N-BaIoT—Network-based detection of IoT botnet attacks using deep autoencoders, IEEE Pervasive Comput. 17 (3) (2018) 12–22, http://dx.doi.org/10.1109/MPRV.2018.03367731.

[177] N. Koroniotis, N. Moustafa, E. Sitnikova, B. Turnbull, Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-IoT dataset, Future Gener. Comput. Syst. 100 (2019) 779–796, http://dx.doi.org/10.1016/j.future.2019.05.041.

[178] S. Garcia, A. Parmisano, M.J. Erquiaga, IoT-23: A labeled dataset with malicious and benign IoT network traffic, 2020, http://dx.doi.org/10.5281/zenodo.4743746.

[179] N. Moustafa, A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets, Sustainable Cities Soc. 72 (2021) 102994, http://dx.doi.org/10.1016/j.scs.2021.102994.

[180] N.S. Almakhdhub, A.A. Clements, M. Payer, S. Bagchi, BenchIoT: A security benchmark for the internet of things, in: 2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), IEEE, 2019, pp. 234–246.

[181] N. Dinh, S. Lim, Performance evaluations for IEEE 802.15. 4-based IoT smart home solution, Int. J. Eng. Technol. Innov. 6 (4) (2016) 274.

[182] R.M. Savola, P. Savolainen, A. Evesti, H. Abie, M. Sihvonen, Risk-driven security metrics development for an e-health IoT application, in: 2015 Information Security for South Africa (ISSA), IEEE, 2015, pp. 1–6.

[183] A. Nrithya, Dolphin attack on smart home systems, 2018, [Online; accessed: June 16, 2022]. URL https://github.com/UCLA-ECE209AS-2018W/Aadithya-Nrithya.

[184] Y. Jang, C. Song, S.P. Chung, T. Wang, W. Lee, A11y attacks: Exploiting accessibility in operating systems, in: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, in: CCS '14, Association for Computing Machinery, New York, NY, USA, 2014, pp. 103–115, http://dx.doi.org/10.1145/2660267.2660295.
[185] W. Diao, X. Liu, Z. Zhou, K. Zhang, Your voice assistant is mine: How to abuse speakers to steal information and control your phone, in: Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices, in: SPSM '14, Association for Computing Machinery, New York, NY, USA, 2014, pp. 63–74, http://dx.doi.org/10.1145/2666620.2666623.
[186] S. Runke, V. Hansen, J. Streckert, M. Clemens, K.-U. Rathjen, S. Dickmann, IEMI analysis of critical infrastructures by simulations using a multi-method coupling strategy, in: 2014 International Symposium on Electromagnetic Compatibility, 2014, pp. 1238–1241, http://dx.doi.org/10.1109/EMCEurope.2014.6931094.
[187] Phonchi, Side-channel attack, 2021, [Online; accessed: June 16, 2022]. URL https://github.com/phonchi/awesome-side-channel-attack.
[188] C. Lentzsch, S.J. Shah, B. Andow, M. Degeling, A. Das, W. Enck, Hey Alexa, is this skill safe?: Taking a closer look at the alexa skill ecosystem, in: 28th Annual Network and Distributed System Security Symposium, NDSS, 2021.
[189] E. Oriwoh, M. Conrad, Presence detection from smart home motion sensor datasets: A model, in: E. Kyriacou, S. Christofides, C.S. Pattichis (Eds.), XIV Mediterranean Conference on Medical and Biological Engineering and Computing 2016, Springer International Publishing, Cham, 2016, pp. 1249–1255.
[190] CyberSecurityUP, Awesome hardware and IoT hacking, 2021, [Online; accessed: June 16, 2022]. URL https://github.com/CyberSecurityUP/Awesome-Hardware-and-IoT-Hacking.
[191] N. Kshetri, Can blockchain strengthen the internet of things? IT Prof. 19 (4) (2017) 68–72.
[192] S. Biswas, K. Sharif, F. Li, S. Maharjan, S.P. Mohanty, Y. Wang, PoBT: A light weight consensus algorithm for scalable IoT business blockchain, IEEE Internet Things J. (2019).
[193] D.B. Rawat, S.R. Reddy, Software defined networking architecture, security and energy efficiency: A survey, IEEE Commun. Surv. Tutor. 19 (1) (2016) 325–346.
[194] C. Li, Z. Qin, E. Novak, Q. Li, Securing SDN infrastructure of IoT–fog networks from MitM attacks, IEEE Internet Things J. 4 (5) (2017) 1156–1164.
[195] S. Son, S. Shin, V. Yegneswaran, P. Porras, G. Gu, Model checking invariant security properties in OpenFlow, in: 2013 IEEE International Conference on Communications (ICC), IEEE, 2013, pp. 1974–1979.
[196] D. Sethi, S. Narayana, S. Malik, Abstractions for model checking SDN controllers, in: 2013 Formal Methods in Computer-Aided Design, IEEE, 2013, pp. 145–148.
[197] R. Skowyra, A. Lapets, A. Bestavros, A. Kfoury, A verification platform for sdn-enabled applications, in: 2014 IEEE International Conference on Cloud Engineering, IEEE, 2014, pp. 337–342.
[198] Y. Li, M. Chen, Software-defined network function virtualization: A survey, IEEE Access 3 (2015) 2542–2553.
[199] S. Lal, T. Taleb, A. Dutta, NFV: Security threats and best practices, IEEE Commun. Mag. 55 (8) (2017) 211–217.
[200] J. Bugeja, A. Jacobsson, P. Davidsson, On privacy and security challenges in smart connected homes, in: 2016 European Intelligence and Security Informatics Conference (EISIC), 2016, pp. 172–175, http://dx.doi.org/10.1109/EISIC.2016.044.
[201] N. Bradley, M. Alvarez, J. Kuhn, D. McMillen, IBM 2015 Cyber Security Intelligence Index, IBM, 2015.
[202] M. Rahimi, M. Songhorabadi, M.H. Kashani, Fog-based smart homes: A systematic review, J. Netw. Comput. Appl. (2020) 102531.
[203] P.K. Sharma, M.-Y. Chen, J.H. Park, A software defined fog node based distributed blockchain cloud architecture for IoT, IEEE Access 6 (2017) 115–124.