



Review article

Landscape of IoT security

Eryk Schiller*, Andy Aidoo, Jara Fuhrer, Jonathan Stahl, Michael Ziörjen, Burkhard Stiller

Communication Systems Group CSG, Department of Informatics IfI, University of Zürich UZH, Binzmühlestrasse 14, CH-8050, Zürich, Switzerland



ARTICLE INFO

Article history:

Received 25 April 2021

Received in revised form 6 March 2022

Accepted 20 March 2022

Available online 12 April 2022

Keywords:

IoT

Security

Taxonomy

Attack vectors

Countermeasures

GDPR

ABSTRACT

The last two decades have experienced a steady rise in the production and deployment of sensing-and-connectivity-enabled electronic devices, replacing “regular” physical objects. The resulting Internet-of-Things (IoT) will soon become indispensable for many application domains. Smart objects are continuously being integrated within factories, cities, buildings, health institutions, and private homes.

Approximately 30 years after the birth of IoT, society is confronted with significant challenges regarding IoT security. Due to the interconnectivity and ubiquitous use of IoT devices, cyberattacks have widespread impacts on multiple stakeholders. Past events show that the IoT domain holds various vulnerabilities, exploited to generate physical, economic, and health damage. Despite many of these threats, manufacturers struggle to secure IoT devices properly.

Thus, this work overviews the IoT security landscape with the intention to emphasize the demand for secured IoT-related products and applications. Therefore, (a) a list of key challenges of securing IoT devices is determined by examining their particular characteristics, (b) major security objectives for secured IoT systems are defined, (c) a threat taxonomy is introduced, which outlines potential security gaps prevalent in current IoT systems, and (d) key countermeasures against the aforementioned threats are summarized for selected IoT security-related technologies available on the market.

© 2022 The Author(s). Published by Elsevier Inc. This is an open access article under the CC BY license (<http://creativecommons.org/licenses/by/4.0/>).

Contents

1.	Introduction.....	2
2.	Methodology.....	3
3.	Internet-of-Things (IoT).....	3
3.1.	Industrial Internet-of-Things (IIoT).....	3
3.2.	Internet of Medical Things (IoMT).....	3
3.3.	Smart cities.....	3
3.4.	Smart homes.....	3
4.	Security background.....	3
4.1.	Introduction to security.....	3
4.2.	Security terminology.....	4
5.	Networking background.....	4
5.1.	Network topologies.....	4
5.1.1.	Point-to-point connection.....	4
5.1.2.	Daisy chain.....	4
5.1.3.	Star topology.....	4
5.1.4.	Mesh topology.....	4
5.1.5.	Gateway nodes.....	4
5.2.	Data transmission.....	5
5.3.	Protocols.....	5
5.3.1.	TCP/IP.....	5
5.3.2.	6LoWPAN.....	5
5.3.3.	Thread.....	5
5.3.4.	BLIP.....	5

* Corresponding author.

E-mail addresses: schiller@ifi.uzh.ch (E. Schiller), andy.aidoo@uzh.ch (A. Aidoo), jara.fuhrer@hotmail.com (J. Fuhrer), jonathan.stahl@uzh.ch (J. Stahl), michael.zioerjen@uzh.ch (M. Ziörjen), stiller@ifi.uzh.ch (B. Stiller).

5.3.5.	CoAP & MQTT	5
5.3.6.	Grafana	5
6.	IoT architectures	5
7.	Challenges in IoT security	6
7.1.	Background	6
7.2.	IoT security aspects	6
7.3.	Securing a heterogeneous distributed system	7
7.3.1.	Usability vs. security	7
7.3.2.	Constrained resources limit security	7
7.3.3.	Short time-to-market vs. security	7
7.3.4.	Availability and ubiquity	7
8.	Security objectives, threats, and threat taxonomy for the IoT domain	8
8.1.	IoT security objectives	8
8.1.1.	Identification	8
8.1.2.	Authentication and authorization	8
8.1.3.	Integrity	8
8.1.4.	Confidentiality	8
8.1.5.	Privacy	8
8.1.6.	Availability	8
8.1.7.	Non-repudiation	8
8.1.8.	Security objectives compilation	8
8.2.	IoT security threats	8
9.	IoT security landscape	9
9.1.	New IoT device hardware	9
9.1.1.	Hardware security module	10
9.1.2.	Secure element	10
9.1.3.	ARM TrustZone	10
9.2.	Network management	10
9.3.	Authentication	10
9.4.	Privacy policies	11
9.4.1.	Consent	11
9.4.2.	Data minimization	11
9.4.3.	Transparent processing	11
9.4.4.	Data breach reporting	11
9.4.5.	Privacy by design and data security	11
9.5.	Forensics	11
9.6.	Life-cycle management	12
9.7.	Ongoing projects and existing guidelines	12
9.7.1.	IETF	12
9.7.2.	GSMA	13
9.8.	New products for increased IoT security	13
9.8.1.	Software	13
9.8.2.	Hardware and firmware	13
9.8.3.	Service and cloud	14
9.8.4.	Home use	14
9.9.	IoT business outlook	14
10.	Discussion	14
11.	Summary and conclusions	15
	Declaration of competing interest	15
	Acknowledgments	15
	References	15

1. Introduction

The Fourth Industrial Revolution, also commonly referred to as Industry 4.0, is expected to alter almost every business sector with unprecedented velocity fundamentally. Industry 4.0 is characterized by the blurring lines between physical and virtual reality. One cornerstone of this technological revolution is Internet-of-Things (IoT) [1]. IoT is defined as an overall, intelligent system with comprehensive awareness, reliable transmission, and intelligent processing of data [2].

With the increasing ubiquity of IoT devices, the number of devices to be used in potential attacks increases, respectively [3,4]. Currently, around 31 billion “things” are connected, and it is estimated that this number will rise to 75 billion by 2025 [4,5]. Most of these devices used by private consumers are Smart Home devices, like TVs, set-top boxes [6], entertainment systems, speakers

or lighting, and heating sensors [7]. These apparatuses can theoretically monitor people without drawing attention from their victims. Consumers expect monitoring activities, such that gadgets can provide their intended functionality. E.g., an intelligent light system is expected to listen to voice commands. However, a user cannot control that only commands are being processed. The private conversations may be listened to, processed, or stored.

Due to the more widespread application of IoT, concerns about its security are well known today. More traditional Information Technology (IT) security goals consisted mainly of guaranteeing confidentiality, integrity, and accountability of systems and messages. However, these traditional measures show measurable limitations, when applied to IoT devices, e.g., due to their computing power typically being insufficient for long(er)-lasting operations. Furthermore, scalability concerns emerged due to IoT devices' vast interconnections. IoT security is critical in the context of these example applications as outlined above: without

valid security models suitable for IoT, full user acceptance cannot be gained. Thus, trust must be established first [8].

To ensure a wide-spread adoption of secured IoT products and applications, an effort has to be invested in structuring the landscape of IoT security. Thus, based on a summary of major security objectives that have to be respected in the design, specification, and implementation phases of IoT applications, this survey positions IoT-related threats within a well established IoT architectural model to focus the attention of IoT developers on major attacks vectors that may emerge on different level of IoT-integrated systems.

To accomplish these objectives, this paper is structured as follows: Section 2 discusses the methodology of this work. While Section 3 explains the basics of IoT, the background on Security is presented in Section 4 and IoT networking is briefly presented in Section 5. Section 6 elaborates on the IoT architectures. While the characteristics of IoT devices are explored in Section 7, the in-depth look at IoT security objectives and the introduction of a new threat taxonomy is performed within Section 8. Section 9 investigates the current market of selected security solutions available and addresses regulations' impacts. Finally, the discussion in Section 10 is followed by a short summary and conclusions drawn in Section 11.

2. Methodology

The methodology of this work is the following. To evaluate IoT security challenges and the threat taxonomy, the authors searched for literature on IoT security. To this end, the keywords *iot* and *security* were used to look for relevant survey papers using several publication databases such as ACM, IEEE, Elsevier, Springer, and MDPI. When these taxonomies were completed, the authors evaluated various techniques presented in those surveys and selected a set of relevant topics they understand are essential for network security, provided using the authors' own experience in the security domain. Furthermore, the authors searched for papers presenting various solutions of high recognition in the domain. Finally, the authors used Internet search engines to look for interesting products in the security domain.

3. Internet-of-Things (IoT)

The first primitive device in this IoT category was a remotely controllable toaster, introduced in 1990 as a proof-of-concept [9]. Ten years later, the first large-scale smart device application was an item identification system based on Radio Frequency IDentification (RFID) [10]. Cisco, IBM, and Ericsson were at the forefront of educating and commercializing IoT for consumers [11]. Some IoT devices have already become the industry standard; mainly thermostats autonomously adjusting temperatures and production line sensors keeping track of machine conditions have been widely adopted [12]. It is estimated that by 2023, machines will materialize half of the Internet-capable devices, while half of the Internet traffic will originate from machine-to-machine connections in IoT [13]. Hundreds of new devices are connected to the Internet every minute [12]. The growth rate of IoT devices deployed is exponential. It is estimated that around 31 billion IoT devices are currently in use, and by the end of this year, another four billion IoT devices will be added, totaling 35 billion. By 2025 this number will have more than doubled, resulting in 75 billion connected IoT devices.

Applications of IoT devices are limitless, hence, the rapid growth of the market as above, which is categorized into four major application domains:

3.1. Industrial Internet-of-Things (IIoT)

IIoT addresses applications in production lines, where machines communicate with each other. They can monitor each other and distribute the workload evenly between them, detect wear, and tear to prevent failure and guarantee constant production, as well as provide real-time production data [14].

3.2. Internet of Medical Things (IoMT)

IoMT primary responsibility is to ensure the continued availability of information [15]. A patient's heart monitor sends information to a health care provider for monitoring. Furthermore, the remote access also allows for a remote configuration. Even a more extensive clientele uses fitness trackers and smartwatches [16]. Such IoMT devices can track sleep patterns, vital data, and physical activity. According to [17,18], both physical activity and sleeping patterns play a fundamental role in preventing chronic diseases and conditions. Thus, health insurance can offer risk-based premiums by leveraging data from wearable IoT devices. Depending on future norms, a health insurance company, which does not leverage IoT devices to mitigate risk, may have an insurmountable disadvantage, which may prevent can from a successful operation on the market [19].

3.3. Smart cities

Smart Cities determine a very influential application category on the society [20]. Caused by the rapid growth of the urban population worldwide, economic growth in cities happens. IoT helps manage this rapid urbanization, since IoT devices in Smart Cities regulate traffic efficiently by recognizing traffic flows and deriving optimal traffic light operations. Additionally, a garbage disposal may be optimized by equipping garbage bins with sensors. Instead of inefficiently driving along streets and collecting every dumpster, only filled containers will be considered for pick-up [21]. Cities collect, by design, a plethora of data ranging from tax payments to water consumption data or building permits. Thus, making such data available shows plenty of benefits: government can become transparent, provide means for innovation, and help unlock trillions in economic value [22].

3.4. Smart homes

The fourth application category is *smart homes*. The aforementioned widely spread thermostat as well as the trailblazer of IoT, i.e., the Internet-capable toaster, belong to this category. Other appliances include smart TVs, connected light bulbs, shutters, door locks, and surveillance [16,23].

4. Security background

Due to the wider interpretation of the term *security*, this work's focus is determined by a short overview and its related taxonomy.

4.1. Introduction to security

The umbrella term *IT-Security* is not static and evolves over time with new technology arriving. In the 1980s, IT security encompassed the goals of ensuring information confidentiality, availability, and integrity [24]. These definitions may be ambiguous, since confidentiality can be applied to the confidentiality of contents or communications on closer inspection. Thus, confidentiality can also be breached, when a third party either gains knowledge of the existence of a communication, its origin, or its

destination. The security goal here is defined as: a message is confidential, if only the sender and receiver know of its existence. It shows integrity, if a message's content is identical for the sender and any receiver. Furthermore, both parties can verify these criteria. The goal of availability specifies that the message is readable by the sender and recipient at any moment's notice.

These goals, however, are not embracing all essential aspects, such that two decades later, accountability was added. A recipient shall be able to demonstrate the origin of the message and vice-versa. Furthermore, the sender of the message cannot send it on behalf of someone else [25]. According to [26], the focus of IT security has shifted from mainly focusing on availability in the early days of computers to guaranteeing confidentiality, integrity, and accountability. Furthermore, detailed security objectives will be covered in Section 8.1.

4.2. Security terminology

In the context of this work, an *adversary* is defined as an entity accessing a system's resource illegitimately [27]. *Malware* is a software to accomplish the goal mentioned above [28].

Generally speaking, a *risk* in IT occurs, when a threat and a vulnerability are paired. Provided that perfect hardware is coupled with perfect software, neither an adversary nor malware would risk an IT system. However, since perfect systems do not exist, IT security measures have to be taken in order to minimize harm [26].

A *threat* is any event having the potential to breach security and cause damage. Its existence requires the capability of execution or favorable circumstances [29]. For instance, the installation of malware by a capable adversary always poses a threat to a system. Nevertheless, it does not automatically become a risk.

Vulnerability exists for an IT system, when a "flaw" in at least either the system's design, its implementation, operation, or management exists [29]. In continuation of the example, to pose a risk, the adversary could exploit the human's most error-prone parameter of a system. By sending malicious e-mails, the adversary could gain system access and introduce malware into the system.

Only when all pre-conditions are met and actions executed, the risk becomes an *attack*, which can be divided into "intent" and "origin". An attack can either alter system resources or gather information from the system by focusing on the intent. The former is classified as an active attack, the latter as a passive one. The origin distinguishes between inside and outside attacks. However, an inside attacker is authorized to access system resources and does it in an unapproved way. Outside attackers do not hold any authorizations to be inside a system [29].

5. Networking background

A network of computers is characterized by an interconnection of at least two autonomous endpoints, synonymous to *node*, which exchange information. The transmission medium is termed a *link*, which can be wired or wireless. A network protocol governs the communication between nodes. Thus, networks offer reliable and flexible resource sharing, as well as communications between users [30].

Telecommunication networks exist in flavors, which can be divided into physical and logical networks [31]. The former focuses on a network of physical entities, including connected switches and routers—this type of network topology used to be the main subject of security research in the past. Currently, robustness and scalability are essential. Therefore, the emphasis is put on the design of logical topologies [32], where information flows from one entity to another, independently of the nature of underlying physical resources.

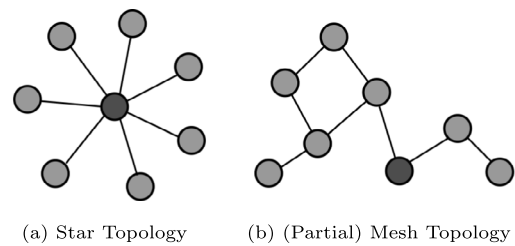


Fig. 1. Most common network topologies also applied in IoT scenarios.

5.1. Network topologies

Existing network topologies are summarized in four major categories, including the specific role of gateway nodes, since these show different impacts in various IoT scenarios.

5.1.1. Point-to-point connection

Nodes connected with a dedicated connection form the point-to-point topology, where nodes act as endpoints and the wire provides a dedicated link between them. In order to function correctly, neither of these endpoints nor the dedicated link may fail.

5.1.2. Daisy chain

When endpoints connect in a series, the resulting network topology is referred to as a *daisy chain*. Such a linear network connects endpoints point-to-point, where one endpoint can act as an IoT monitor. It is typically used in smaller networks due to its cheap installation and expansion. However, troubleshooting is one of its weaknesses, while disrupting one node of a daisy chain can have dramatic impact on the entire network. Furthermore, adding or nodes endpoints can disturb the entire topology.

5.1.3. Star topology

When all nodes are connected to a central gateway (cf. below), the resulting topology is referred to as a *star topology* (cf. Fig. 1(a)). The main advantages of *Star Topologies* are their cost-effectiveness, easiness of deployment, and reliability. Failure or vulnerability of a node does not compromise the entire network. An analogy includes shunt circuits, where a defective light bulb does not prevent other light bulbs from operating. However, the maintenance cost of a star topology is high, and the installation and configuration are difficult.

5.1.4. Mesh topology

A *(Partial) Mesh Topology* is characterized by at least three distinct nodes, where each of these endpoints neighbors with a subset of other endpoints (cf. Fig. 1(b)). Links can be generated dynamically and non-hierarchically [30]. Due to its scalability and reliability, a mesh topology is suitable for the deployment of IoT networks [33]. For instance, Google Nest, Google WiFi, and Google OnHub support WiFi mesh networking [34]. Furthermore, the recent advent of Long Range (LoRa) [35] mesh networks [36] can have a stimulating impact on the development of IoT networks of the mesh topology.

5.1.5. Gateway nodes

Enabling data transmission from one network to another, *Gateways* [37] provide the network with interconnection functionality. In IoT, gateways provide bridges between devices or even subnetworks, while hubs interconnect network segments. Furthermore, gateways can amplify signals to extend the range of a wireless transmission medium and regulate information flows between networks.

5.2. Data transmission

A transmission medium, *i.e.*, the link, is required to transport information in terms of messages from one node to another. Electric cables, optical fiber, radio waves, and light selected according to various criteria lead to different capabilities of transmission links. As one transmission characteristic, bandwidth refers to the data transmission capacity in terms of bits per second. Additionally, especially often in IoT deployments, signal deformation can be caused by noise or medium characteristics, which influence on how much information is lost upon the transmission.

5.3. Protocols

A network of networks is commonly referred to as the *Internet*, where humans and machines communicate with each other while being geographically apart. The transfer of messages follows standardized protocols to provide inter-connectivity between IoT nodes and networks.

5.3.1. TCP/IP

The *Transmission Control Protocol and Internet Protocol* (TCP/IP) is the most widely used protocol on the Internet and breaks up a message into packets to be sent to its destination.

Several problems in the TCP/IP architecture have to be considered in the context of IoT. **The Maximum Transmission Unit (MTU) of 1280 Byte in IPv6 might be too large for low-powered devices providing low MTUs.** Moreover, **TCP offers several features such as transmission reliability, flow control, congestion avoidance, which might be too heavy to be implemented on constrained IoT devices.** Furthermore, while IoT links might be lossy, TCP does not offer good performance, because it assumes that losses are only caused by congestion.

Due to such limited resources, a direct implementation of the TCP/IP stack on an IoT device might be impossible. Wireless Sensor Network (WSN) technologies, including 6LoWPAN, Thread, and BLIP, are examples of resource-efficient solutions and protocols for limited networks [37].

5.3.2. 6LoWPAN

The Internet Engineering Task Force (IETF) formed the IPv6 over Low-power Wireless Personal Area Networks (6LoWPAN) working group [38]. The 6LoWPAN nano stack only requires 4 kByte RAM (Random Access Memory) and enables IPv6 functionality on top of User Datagram Protocol (UDP) to ensure that sensor nodes are compatible with many underlying Physical (PHY) and Medium Access Control (MAC) layers. As a result, RFC 4919 [39] describes the transmission of IPv6 packets over IEEE 802.15.4 networks, RFC 6606 specifies routing [40], RFC 6775 addresses neighbor discovery [41], and RFCs 8066 and 8025 define header handling algorithms [42,43]. Interoperability with IP networks was achieved as a result. Packet fragmentation, reassembling, routing, neighbor discovery, and multicast support are supported by 6LoWPAN. Thus, 6LoWPAN replaces the Network Layer with an Adaptation Layer that supports only 2 to 11 Byte overhead compression of TCP/UDP and IP headers. Furthermore, UDP and TCP are supported at the transport layer, too.

5.3.3. Thread

Thread devices have an IEEE 802.15.4 PHY-compliant interface and show additional support a subset of the IEEE 802.15.4 MAC protocol. Thread also employs 6LoWPAN. Because of the low power consumption, IoT devices may have a weak transmission signal, making communication more difficult. Therefore, Datagram Transport Layer Security (DTLS) [44] is used by Thread Personal Area Networks (PAN) for message confidentiality, which assumes an unreliable transport layer.

5.3.4. BLIP

The Berkeley Low-power IP stack (BLIP) [45] supports a variety of constrained device platforms. Several parts constitute the simplified BLIP stack. The 6LoWPAN lower component compresses headers and divides big packets into several link-layer fragments to comply with a low MTU. The IP Interface provides network services like IPv6 neighbor finding, forwarding, and routing. The Transport Interface supports custom UDP and TCP protocols. And all necessary application-layer protocols are included as applications. BLIP provides addressing, stateless auto-configuration, and header compression for constrained devices, allowing for IP communications.

5.3.5. CoAP & MQTT

The Constrained Application Protocol (CoAP) [46–48] and Message Queuing Telemetry Transport (MQTT) [49] are the two main application messaging protocols used by IoT applications at the Transport layer. Both of these communications protocols were created with low-power IoT devices in mind. CoAP is a service layer protocol designed for internet devices with limited resources, such as wireless sensor network nodes. And CoAP is a message oriented protocol designed to simplify Hyper Text Transfer Protocol-related functionality and adapt it to IoT applications by addressing unique IoT criteria, like low overhead and simplicity. MQTT is a lightweight messaging protocol that uses the publish/subscribe communication pattern for distributed applications to connect embedded devices. Oasis has standardized this protocol, which IBM initially developed.

5.3.6. Grafana

One of the most popular architectures receiving data from IoT devices (*cf.* Fig. 2) is the IoT MQTT protocol coupled to the Graphite open-source data storage platform. The data is displayed through an open-source dashboarding system, such as Grafana, which can retrieve time series and display them [50].

6. IoT architectures

Due to the heterogeneous nature of IoT devices, no standard “construction path” for IoT deployments fits all use cases.

However, several architectures are presented in the literature. One approach divides an IoT architecture into three layers, depending on their characteristics [2,51–53]. Other approaches divide the architecture into more fine-grained layers (*e.g.*, four-layer architectures [54,55] or the seven-layer IoT World Forum Reference Model [56]). Another option of describing and building IoT networks follows the *Fog computing paradigm*, which also makes use of three layers, but applies different concepts to classify devices (*i.e.*, edge, fog, and cloud computing) [57]. For the remainder of this work, the most commonly used three-layer architecture is chosen due to its intuitive nature (*cf.* Fig. 3). Its layers read as follows:

- **Application Layer:** The top layer consists of applications and middleware. Depending on the use case, it can include elements of cloud computing, integrations to other applications, resolution services, or Web services. In general, the layer is responsible for delivering application-specific services to the user [2,51–53].
- **Network Layer:** The middle layer consists of the network required for data transmission between IoT devices, other network devices, or servers. Depending on the use case, different network types, such as mobile communication networks, computer networks, or wireless networks, make use of different protocols (*e.g.*, Constrained Application Protocol (CoAp) or ZigBee) [2,37,51–53]. Since this layer is responsible for the communication between different devices and services involved, this layer is also referred to as the *Communication Layer*.

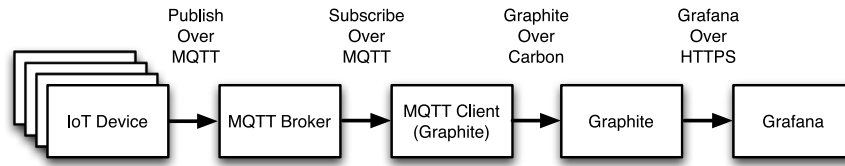


Fig. 2. MQTT with Graphite and Grafana.

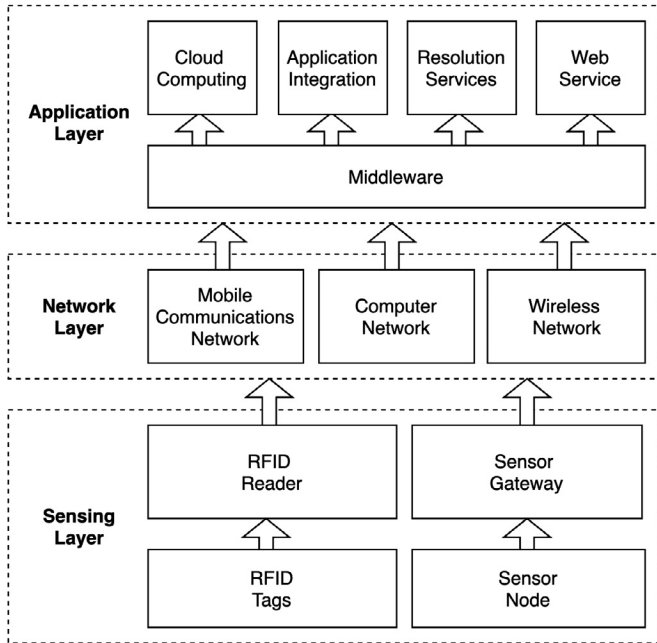


Fig. 3. Three layer architecture of IoT, based on [51].

- **Sensing (or Perception) Layer:** The bottom layer is the physical layer, which consists of all IoT devices (e.g., sensors, RFID readers or tags, and gateways). In many cases, it involves sensors and actuators that are embedded in the environment [2,51–53]. Since this layer mainly embeds hardware, it is referred to as the *Hardware Layer* or *Physical Layer*, too.

7. Challenges in IoT security

To derive the key challenges IoT security faces today, a common background is established first. Based on that, an IoT security analysis is performed, which was extended specifically with a detailed view on heterogeneous distributed systems.

7.1. Background

Considering IoT basics, especially indicating the well-observed migratory path of IoT devices embedded into traditional IT systems and communication networks, securing IoT devices and their operations remains the key challenge.

One of the leading security concerns is IoT devices' weak default credentials. This vulnerability was the entry point for prominent cyberattacks, like the Mirai botnet [58]. Once inside the network, additional devices are infected, which await instructions to commence a Distributed Denial-of-Service (DDoS) attack. One of the premier Web host providers Dyn [59], which hosts well-known Web sites of Twitter, Reddit, GitHub, and Netflix, became a victim of a Mirai attack resulting in the unavailability of the Web sites mentioned above for several hours. Contrary to laptop and desktop computers, many IoT devices operate 24/7

and are, therefore, always available for a botnet attack. Furthermore, many IoT producers want to benefit from the first-mover advantage and, thus, release a user-friendly product lacking security. **Malware in IoT devices mostly remains unnoticed due to a minimal necessity of interactions with user interfaces. These determine major reasons why IoT devices are particularly suitable for creating botnets [58].**

Generally, the consequences of IoT security negligence do not stay in the digital realm. In 2008, a comprehensively monitored pipeline, which transports crude oil from the Caspian Sea to the Mediterranean, exploded without triggering a single distress signal. Immediately after the blast, the organization Partiya Karkerên Kurdistanê (PKK) claimed credit, while official sources blamed malfunctions. According to [60], however, similarly to the Mirai botnet [58] the adversary's entry points were cameras. Therein after, the pipe pressure was probably increased, while simultaneously manipulating the data displayed in the operational control room, until the explosion occurred [60]. In 2010 the computer worm Stuxnet was discovered. This cyberattack is suspected to be a collaborative effort between intelligence organizations to prevent Iran from producing weapons-grade uranium. The precision of this cyberattack made the computer worm to exploit zero-day vulnerabilities to cause physical degradation in machines, which were connected in a completely isolated network [61]. These cases serve as powerful precedents from a time when the number of IoT devices was way smaller.

7.2. IoT security aspects

Security is one of the key concerns within IoT, cf. [53,62–64]. While security is important for any IT, it is even more critical for IoT. [65] summarize three reasons: Foremost, IoT systems, which are out of control, cannot only jeopardize the users' privacy, but also can cause physical harm, when sensors, actuators, or other connected devices are used maliciously. Secondly, they point out a risk for manufacturers, since once attackers could get access to sensitive information or proprietary assets through the IoT system, manufacturers lose valuable information and damage their reputation. Thirdly, due to the high interconnectivity of IoT systems, the impact of an attack goes beyond a specific device or network. In this sense, the saying "A chain is as strong as its weakest link" is perfectly applicable; the IoT network is as secure as its weakest device.

The major objectives of IoT security are to ensure privacy, confidentiality, integrity, and availability of these services offered [3, 53,65]. Further details are part of Section 8.1 below. Another crucial aspect has been added to the list within the last years: financial incentives. [66] references a Ponemon Institute's study (a research center devoted to privacy and data protection [67]), where data breach costs are estimated on an average of 141 US\$ per data record or around 3.6 million US\$ per incident. This massive amount is needed to analyze the harm caused by a breach, to fix the actual breach, and also for insurance protection, compliance, or reputation recovery [68]. Hence, IoT security is not only applied to meet the above security objectives. It becomes an increasingly important part of a company's business strategy to prevent such high data breach costs and the reputation damage, which inevitably follows.

Despite economic benefits [66], and the particular importance of IoT security [65], the IoT industry and its devices are far away from being secure. A study led by Hewlett-Packard indicated that around 70% of the generic IoT technologies contain “some” security vulnerability, such as unencrypted data transmissions or very basic passwords [63,69]. [63] expects security to be one of the fundamental design decisions of IoT systems, yet sees insecure devices brought to market by vendors, who does not put sufficient effort in securing their technology. This is explained with the particularity of the IoT sector and its devices: customers want user-friendly, battery-efficient, and good-looking products—and all this as quickly as possible. Several features can be deducted from these requirements, which are particularly relevant for IoT devices. These features differentiate an IoT device from a traditional IT device, like a laptop or server. Several research attempts, including [3,53,63,65,70,71] attribute the reasons why it is hard to secure IoT devices according to these characteristics, while they identified characteristics that sometimes make it even impossible to apply traditional security measures to IoT devices, too.

7.3. Securing a heterogeneous distributed system

In contrast to standard IT systems, which are often considered as “monolithic apparatuses”, a novel IoT network consists of many “connected microcomputers” [63, p. 85]. Regrettably, until now, most IoT manufacturers have failed to treat it as such. Measurably unique security requirements and characteristics have to be incorporated within the design process of IoT devices. However, manufacturers have often neglected these. The consequences are IoT networks, which are vulnerable to inevitable cyberattacks.

IT pioneer Peter Neuman claimed, “You can’t add security into something that isn’t designed to be secure”. [63, p. 85]. Based on the literature evaluated, this reveals true for very many IoT technologies. Thus, it is essential to determine IoT’s characteristics, outline major difficulties to protect IoT devices, and emphasize the special attention IoT needs, since it cannot be equated to “regular” IT.

Interconnectivity and heterogeneity go hand in hand. The IoT network consists of numerous integrated and heterogeneous devices, which actively share data amongst each other [62,72]. All these open connections create multiple access points for potential attackers to exploit existing vulnerabilities [3]. Participating entities are heterogeneous in terms of their communication patterns, policies, protocols, features, manufacturers and, of course, their security standards. Also, they are often geographically dispersed, which means that regulations from different countries might apply [3,65].

These characteristics of IoT networks do not favor comprehensive security standards and countermeasures against cyberattacks. Nevertheless, various working groups started to design guidelines and best practices that manufacturers could use as a reference point. They create new protocols adapted to IoT particularities with the goal of making them secure (cf. Section 9).

7.3.1. Usability vs. security

Customers desire user-friendly products [63]. The initial setup has to be quick and onboarding of new devices straightforward. The device should be easy to use and appealing to the eye. These requirements are in contradiction to security measures. Passwords that protect the device and the network against unauthorized access are often annoying and interrupt smooth usage. Hence, manufacturers keep such “enforced interactions” to a minimum and usability high [73].

If password authentication is still needed, users are asked to define one upon the initial setup. Not too seldom, a simple,

already used password is chosen, or, even worse, the default password is kept. Dictionary-based as well as more sophisticated attacks are able to guess these passwords [74]. Additionally, selected manufacturers hard code passwords to keep the disruption low and minimize the effort needed to set up a device. These highly insecure default settings make the IoT device vulnerable by design [55,69].

The report [6] published in 2017 states that more than 60% of IoT applications have been used by the consumer segment, while the business sector accounted for the rest. Although businesses might employ IT specialists to evaluate and finally bootstrap IoT devices and networks, private consumers very likely lack expertise and often are not as tech-savvy. Hence, these products must be easy to use and set up for the broader public, which results in the renunciation of tough security measures [73].

7.3.2. Constrained resources limit security

Security measures are typically based on “expensive” schemes, like encryption and signing, without considering the resource consumption explicitly [75]. IoT devices, however, are resource-constrained in terms of computing, memory, storage, networking, and energy, making it challenging to secure them properly [3,53,70]. IoT devices, usually compact and light, do not store a large battery. Additionally, since they need to operate autonomously, not requiring a human intervention to replace a battery frequently, they have to limit the power consumption and be operated energy-efficiently [71,75,76]. Furthermore, IoT devices also need to operate resource-saving regarding memory. If there is no space for a long-lasting battery, there is often neither space for more significant memory. The same holds for processors: the complexity of CPUs and sensors is limited due to space and weight. As IoT deployments already have to be conducted in lossy and low-bandwidth communication channels, there is limited capacity for heavy overhead [65,71,72,76].

Such resource limitations prevent traditional security measures on IoT devices because due to resource-constrained devices are particularly susceptible to exhaustive attacks [65].

7.3.3. Short time-to-market vs. security

The IoT world is rapidly changing. Vendors have to deliver their products fast to keep up with the competition. They do not take time to develop sophisticated security measures and instead apply quick security fixes if necessary [63]. In doing so, they produce commercial off-the-shelf products, which are not well-developed and secured [63,72], but easy to set up and affordable. Instead of being a “fundamental design focus” [63, p.84], IoT security still relies on technology and protocols developed for the Internet. However, since the Internet cannot be equated to the IoT domain, integrated systems interacting closely with people, possibly causing severe harm, need serious reconsideration. Furthermore, a well-secured, but possibly expensive product would likely not be successful. Customers command good bargaining power, the required time-to-market is short (i.e., minimization of the time that passes until an idea becomes a product ready for the market), and additional security costs are disproportional to the cost of the device itself [63,70].

7.3.4. Availability and ubiquity

IoT devices are constantly connected to the Internet. They are not like laptops or phones, which are shut down entirely from time to time [58]. Hence, IoT devices constitute a reliable target for attackers, always available and interconnected. Additionally, IoT devices seem to be everywhere. They create massive networks with access to several areas, such as households, companies, transportation, and factories, and they are becoming accessible simultaneously due to the deployment of IoT devices [3,58].

Table 1
Security objectives in IoT according to literature.

Security objective	Literature references
Integrity	[55,65,77,78,80] [3,54,71,83,84]
Confidentiality	[55,71,77,80,81] [3,54,83,84]
Authentication	[55,65,77,79,81] [3,54,78,83]
Privacy	[65,71,77–79] [54,83]
Availability	[55,65,71,77,80] [3,84]
Authorization	[3,55,65,77–79]
Non-repudiation	[3,77,78,81]
Identification	[78,79,81]
Reliability	[54,79,81]
Freshness	[77]
Access control methods	[55]
Soundness	[84]

8. Security objectives, threats, and threat taxonomy for the IoT domain

Based on the literature-driven introduction of security objectives that need to be achieved along with their definition in the context of IoT, the threat taxonomy provided below aggregates the findings from a holistic perspective on IoT threats.

8.1. IoT security objectives

The characteristics of IoT devices introduced above expose them to numerous threats. Table 1 contains those security objectives relevant in the IoT domain according to existing literature. It is presented in the context of a short definition for each objective [55,65,77–81].

8.1.1. Identification

All entities in an IoT system need to be able to identify other participants. They need to be aware of other entities in the network. Furthermore, entities need to distinguish friendly from potentially malicious entities. In most cases, IoT devices will reside in a particular context, e.g., belong to a group, are located in a particular building, owned by a specific entity. Therefore, identification refers to the process of claiming a given identity [82].

8.1.2. Authentication and authorization

Before access to a restricted resource is allowed (e.g., sensitive information) sensing devices, users, and gateway nodes must be authenticated, i.e., their identity must be verified. It must be ensured that they are who they claim to be [85].

After the identity has been verified, it must be ensured that the entity under consideration is allowed to access the data, resources, or applications within the system. In the domain of IoT, access to a given resource might depend on additional factors, such as the identity of the owner of the device, i.e., providing more information on people with certain roles, or the location, i.e., checking whether a user is accessing the device locally or remotely [86].

8.1.3. Integrity

It must be ensured that the data or message was not changed, i.e., modified, altered, or destroyed, during its exchange and transmission, storage, and processing [54].

8.1.4. Confidentiality

Secret information needs to be protected from unauthorized disclosure, either during transport and within a storage [87,88].

8.1.5. Privacy

During the handling, processing, storing, and deletion of data, it must be ensured that the rights of individuals regarding the use of personal information are appropriately addressed. This usually involves adhering to contracts, policies, and applying a governing regulation or law, e.g., within Europe the General Data Protection Regulation (GDPR) in force since 2020 [89].

8.1.6. Availability

The system and its services have to be available when required. Thus, availability refers to the probability that a system (or component) is operational at a specific point in time. As proposed by [90], this incorporates both reliability, i.e., meeting certain performance standards in a given context, and maintainability, i.e., the ability to uncouple, fix, and modify components without obstructing the service and violating predefined thresholds.

8.1.7. Non-repudiation

With malicious but initially not visible intent, any entity should not be able to hide their actions [77]. Thus, non-repudiation ensures that no entity can claim that a transaction did not happen when it, in fact, did or vice versa. It ensures that circumstances can be resolved, where different parties in the system hold different views of that what happened, e.g., during a network failure [91].

8.1.8. Security objectives compilation

As shown in Table 1, the literature does not offer a clear consensus about the essential security objectives in IoT. This is partially due to overlapping terms and definitions, e.g., the term *Authentication* sometimes also includes *Identification* seeing the latter as a prerequisite of the former. Literature also does not always provide a succinct definition of terms used for objectives, complicating the comparison of findings. Some papers introduce even new security objectives, such as *Freshness* (confirmation that the message is fresh and any adversary cannot replay old messages), *Access Control Methods*, or “Soundness” (in impersonification attacks, preventing a verifier from assuming false statements as truth). This is not thoroughly elaborated in this review due to space.

8.2. IoT security threats

Specific existing taxonomies classify IoT security threats according to the layered IoT architecture [55], others base their taxonomy on a one-dimensional list of threats and countermeasures [83]. To aggregate these findings of existing literature, the taxonomy proposed here is built on top of the three-layer IoT architecture (cf. Section 6). Although this architecture has been criticized for not being able to capture all nuances in IoT systems [52,55], it serves as a common denominator for taxonomies that involve more layers, e.g., the five-layer taxonomy proposed by [81] or the four-layer taxonomy proposed by [92], and, thus, it allows for the incorporation of results from these approaches as well. An IoT system usually consists of different devices with different capabilities that make use of a diverse set of communication protocols (cf. Section 6). Furthermore, various interfaces are required to enable services that use aggregated data collected within the system. Therefore, it is not sufficient to implement security measures based on traditional IT network solutions [53]. The Open Web Application Security Project (OWASP) published

Table 2
Taxonomy of threats and attacks in IoT according to literature following the Three Layer Architecture.

Layer	Attack	Source
Application	Data modification	[55]
	Software reverse-engineering	[65]
	Firmware	[65]
	Elevation of privilege	[65]
	Denial-of-Service (DoS)	[65,77,79,80,92]
	Many logged-in users with the same credentials	[77]
	Stolen-verifier	[77]
	Stolen/lost smart card	[77]
	Password guessing	[77]
	Password change	[77]
	Buffer overflow	[65] [53]
	Impersonation	[77]
	Memory corruption	[80]
	Code execution	[80]
	Structured Query Language (SQL) injection	[53,80]
Network	Cross-site scripting (XSS)	[80]
	Cross-site request forgery (CSRF)	[80]
	Collision	[81]
	Exhaustion	[81]
	Unfairness	[53,81]
	Spoofed, altered, or replayed routing information	[53,81]
	Internet Protocol (IP) spoofing	[55]
	Side channel	[53,55,65]
	Distributed Denial-of-Service (DDoS)	[53,55,65]
	Selective forwarding	[53,65,81]
	sinkhole	[53,65,81]
	Sybil	[53,65,77,81]
	Wormhole	[65,77,81]
	Hello and session flooding	[53,81,92]
	Acknowledgment spoofing	[81]
Sensing	Internet, generally protocol mis-configurations	[80]
	Synchronization	[53,81]
	Replay	[55,77,92]
	Man-in-the-middle	[55,65,77]
	Eavesdropping	[53,65,79]
	Jamming	[53,81]
Sensing	Malicious substitution	[65]
	Tampering/physical damage	[55,79,81]
	Node capture	[65,77,79]
	Cloning/device replication	[65,77]

guidelines for developers and manufacturers on how to secure IoT systems [69]. However, these guidelines focus on the most common vulnerabilities and do not provide an exhaustive list of potential threats or attack vectors in IoT systems.

In contrast to these broadly applicable security guidelines provided, other approaches list threats and attacks based on specific IoT use cases, e.g., smart water systems [3] or smart grids [93]. However, these approaches are limited, since how such an approach could be applied to other domains and use cases is not well described. A threat taxonomy proposed by [64] on one hand incorporates different perspectives, such as identity management, storage management, and physical threats, but on the other hand only lists a few threats for each perspective, thus, being considered of not complete.

Therefore, the threat taxonomy proposed herewith in Table 2 provides a holistic view by incorporating threats and attack vectors listed by those papers investigated. It categorizes threats based on the three-layer IoT architecture and provides references to existing literature, where these threats are examined further, partially detailed in the context of IoT. Although threat lists will never be exhaustive, this taxonomy contains way more threats than existing taxonomies. This new taxonomy also emphasizes that IoT security needs to be addressed from multiple perspectives, and that it is not sufficient to focus on the IoT device itself. It also highlights the heterogeneous threat nature: threats involve physical access to the device, e.g., tampering or physical damage, whereas others focus on software running on the application layer, e.g., SQL injection. This investigation emphasizes the

urgent need for mature security guidelines and solutions focusing on the holistic nature of the IoT system and not just on individual components.

9. IoT security landscape

While the thread taxonomy pictures concerns from outside the technical solution itself, a broader overview of different types of security mechanisms being applicable in turn is essential in terms of countermeasure options. Thus, firstly modifications on IoT devices in terms of hardware are described, and secondly security mechanisms are summarized that play a key role in the security landscape.

Thirdly, a selection of new products supporting IoT security is outlined non-exhaustively. This serves as a sample on diverse collections of products, such that a selection of solutions as countermeasures can serve different approaches. The selection of products and product categories was defined based on the main distinction between products in the *Corporate or Public* category and products designed for *Private* use. Within the corporate and public sector, *Software*, *Hardware/Firmware*, and *Service/Cloud* solutions for IoT are distinguished. Since the market for IoT security solutions in the *Private* category is not as mature, not as many different products exist.

9.1. New IoT device hardware

IoT devices as of the recent generations are currently undergoing a radical shift to support advanced security features,

while at the same time required mechanisms are currently being integrated with microcontrollers already on the hardware level itself.

9.1.1. Hardware security module

Because easily accessible IoT devices are vulnerable to physical attacks, tamper-resistant hardware security modules are required to secure information, such as cryptographic keys and operations like data encryption or PIN verification. A Hardware Security Module (HSM) is a physical entity that adds an extra layer of protection to cryptographic keys, trade secrets, and other sensitive applications or data [94].

9.1.2. Secure element

Secure Elements perform cryptographic operations in hardware, allowing cryptographic algorithms to be executed quickly and efficiently. Secure elements also provide tamper-proof memory for securely storing cryptographic data [95]. Furthermore, since microcontrollers begin to provide cryptographic operations directly in hardware, the performance of cryptographic primitives may increase by many orders of magnitude, allowing several instances of the Digital Signature Algorithm (DSA) of a high level of security executed per second. Therefore, Secure Element is considered essential for successfully integrating IoT applications with the Distributed Ledger Technology (DLT), providing enhanced security to IoT data streams such as authenticity, non-repudiation, or immutability [96,97].

9.1.3. ARM TrustZone

ARM TrustZone [98] has emerged as a critical hardware mechanism that allows for the provisioning of a Trusted Execution Environment (TEE) in which essential applications can run securely. A TEE determines an isolated environment, where trusted applications can run without interruption from the local (untrusted) operating system. TEE's security characteristics ensure confidentiality and integrity of computations performed within. A TEE abstraction also defines mechanisms for a secure provisioning of code and data (including cryptographic keys) into the TEE and trusted channels for obtaining results of computations and errors to guarantee isolated execution, thus, improving overall security, privacy, confidentiality, and data integrity.

9.2. Network management

The management of an IoT device through a dedicated client is cumbersome, if many devices have to be reconfigured at the same time, e.g., when an administrator needs to react to a threat by shutting down services with a vulnerability. Network management offers solutions to this problem by offering a unified centralized management of many devices.

For instance, NETCONF (Network Configuration Protocol) [99] is a network management protocol that allows a Network Management System (NMS) to transmit, change, and delete network device configurations. On network devices, standard Application Programming Interfaces (API) are accessible so that the NMS may manage devices using NETCONF. NETCONF uses Extensible Markup Language (XML)-based data encoding and communications between a client and a server for the configuration of data and protocol messages, implemented using a regular Remote Procedure Call (RPC). Furthermore, NETCONF uses Yet Another Next Generation (YANG) [100] to model network element configuration and status data. YANG organizes data descriptions into tree structures and includes a type system that may be extended. YANG specifies a formal separation of state and configuration data, and a range of syntactic and semantic constraints. Modules

provided in YANG gather data definitions and specifying features for extension as well as reuse.

NETCONF over CoAP closely follows the client/server communication using the REST architecture [101], in which a client initiates the connection and requests functionality from a server. This is a communication method that can only scale, if the server has the capacity to handle all client requests. M4DN.IoT is an example platform heavily re-using this architecture, depending on CoAP and NETCONF [102].

A communication style based on the publish/subscribe pattern may be a better fit for a communication system with a server of constrained resources. Thus, [103] presents a framework for dynamically constructing a YANG data model for the entirety of a controlled IoT domain using domain-specific data. The data within the domain is acquired through the Message Queuing Telemetry Transport (MQTT)-based service with the control plane being tuned to a specific topic, which is responsible for both network discovery and control. This allows for a centralized control of several devices in the domain from a server, which does not possess elevated resources. It is worth noting that when the number of devices changes (i.e., devices frequently join and leave the domain at higher churn rate), the framework will automatically adapt to the dynamic situation.

9.3. Authentication

Authentication plays a crucial role in providing security, privacy, and confidentiality of information in IoT systems [85]. One (or a mix) of hash, symmetric, or asymmetric cryptographic algorithms can be used in identity-based authentication techniques. Authentication is performed using various context-based sources on different user/device characteristics, such as physical (i.e., biometric data based on an individual's physical traits, such as fingerprints, hand geometry, retinal scan) or behavioral characteristics, i.e., biometric based on an individual's behavioral traits, such as keystroke dynamics or gait analysis.

The authentication on IoT devices should be provided based on hardware-based authentication, in which the authentication procedure may need physical device attributes or the hardware itself. On one hand, it might be implicitly hardware-based, which uses the hardware's physical properties, such as a Physical Unclonable Function (PUF) or the True Random Number Generator (TRNG), to improve authentication. On the other hand, explicit hardware-based authentication relies on a Trusted Platform Module (TPM), a chip (hardware) that stores and processes credentials (e.g., keys, certificates) used for hardware authentication.

In the process of authentication, tokens might be used. In token-based authentication, a user/device uses a server-generated identity token (data), such as the OAuth2 protocol or open ID [104]. In non-token based authentication, e.g., Transport Layer Security (TLS) or DTLS, entails the usage of credentials (username/password) every time data must be sent [44,105].

The authentication procedure can be based on one-way authentication, i.e., in a case when two parties want to communicate, only one of them will authenticate itself to the other, leaving the other unauthenticated. Secure authentication can go in both directions, when both entities mutually authenticate each other. Finally, the three-way authentication can be used when a central authority authenticates the two parties and facilitates mutual authentication.

An architecture for authentication can be distributed, in which the communication parties use a distributed direct authentication approach. In a centralized approach, authentication credentials are distributed and managed by a centralized server or a trusted third party. Furthermore, on one hand, the architecture of an authentication technique can be hierarchical. Then, the authentication mechanism is handled using a multi-level design. On the

other hand, the authentication mechanism can be handled flatly, with no hierarchical architecture.

In terms of a decentralized authentication, open identity standards, such as on open identity standards by the World Wide Web Consortium (W3C), i.e., *Decentralized Identifiers* [106] and *Verifiable Credentials* (VC) [107], promote interoperability. The possibility of identification of all responsible entities provides support for accountability.

An Identity or IoT Device Owner can manage multiple public or private DIDs (Decentralized Identifier) derived from public keys and/or user attributes or based on physical device fingerprinting for IoT devices. Such identifiers may be ephemeral—generated for a single interaction between a person or a device and a service, which enhances security and privacy (by avoiding tracking).

The architecture may take advantage of the Self-Sovereign Identity (SSI) by storing Public DID Documents (DDO) containing DIDs, public keys, and service endpoints, or private keys as VCs. The SSI approach requires a public storage for handling and discovering DIDs and DDOs. The first SSI implementations build on permissioned (Sovrin [108], uPort [109]), or permissionless Blockchains (BC) (Bitcoin in Microsoft's ION [110]). However, BCs are immutable, so they might be not well suited for DIDs and DDOs, which may need frequent updates or canceling.

9.4. Privacy policies

Several solutions for IoT threats are available on the market. However, the market is not the sole actor addressing security concerns. In recent years, new regulations have been established that also impact the IoT domain and address security concerns from a different angle. With the widespread use of IoT technology and its impact on everyday life, the need for specific regulations is growing [111], since billions of sensors deployed, tracking every single movement, and noticing every single change leads to the massive information: “Who we are, where we are, what we do and how we do it” [66, p. 1]. IoT devices collect a vast amount of data. Thus, it is essential to look at how IoT can be secured sufficiently and how data handling and processing needs to be governed.

Recent legislation with far-reaching consequences is the GDPR. GDPR's main objective is to protect and regulate the data privacy of European Union (EU) citizens. Therefore, highly sensitive data collected by IoT devices must be subjected to the GDPR as well. However, as [66] points out, there are several hurdles in applying GDPR to the IoT environment. Subsequently, principles of GDPR and challenges associated with it are discussed.

9.4.1. Consent

GDPR states that data subjects, i.e., natural persons, have to be able to control which data is collected about them and that they can forbid that collection at any time [112]. Thus, the question arises, how such a rule can be applied in the domain of IoT. For example, what happens, when a person visits a friend and the smart lock at the entrance collects video footage? Could guests deny the collection of their data during their visit? It seems that current systems still do not provide such kind of control [66]. Even further complication arises when IoT devices are placed in public areas. People can be tracked without even being aware of the presence of monitoring devices. Another use case may include third parties when people are within reach of sensors only for a short time, e.g., when people travel in the train next to a person with IoT devices on them. Obtaining consent from third parties is even more difficult than from active owners of IoT devices [66].

9.4.2. Data minimization

The purposes of limitation and data minimization are principles restricting data collection in general. Data should only be

collected for a specific purpose, and only as much as needed to fulfill this given purpose [112]. An example, IoT often violates those principles is Smart Home systems, when sensors constantly capture audio to recognize user commands such as “Turn on the light”. However, while light is not needed for several hours during the day, IoT devices might still be constantly listening to voice commands.

9.4.3. Transparent processing

Transparent processing refers to the user's capability to observe how the data is handled. For example, how many times a certain fact was recorded, and where and through which channels it has been sent [66]. However, users (and passively concerned people) of IoT technology usually are not informed about third parties, nor can manufacturers be entirely sure how data is handled. Data is often passed from one device to another before arriving at the final destination, where it is stored persistently. Since GDPR's transparency also means the “Right to be forgotten”, i.e., a person can at any time demand from a company to erase all their personal data [112]. In turn, the company has to track, where all personal records are stored and remove these data identified, which might become a challenging task or is even practically impossible [66].

9.4.4. Data breach reporting

According to the GDPR, companies must report a data breach within 72 h after becoming aware of it. This rule is challenging, especially within IoT environments [66]. Finding and assessing a breach among hundreds or even thousands of interconnected devices requires the close cooperation of all stakeholders and vendors. Given the myriad of devices, this process might be almost impossible in reality.

9.4.5. Privacy by design and data security

Privacy by design is accomplished, when users do not have to change default settings to protect their privacy. OWASP criticizes that this is not the case for most IoT devices [69]. Furthermore, the GDPR demands that vendors apply all necessary measures to protect users' privacy and confidentiality. Taking the characteristics above of IoT devices into account, especially limited resources, the deployment of such effective security mechanisms happens to be rather difficult [66].

The European Union's demands for more stringent rules in the IoT environment is complemented by the US Federal Trade Commission (FTC), which has also identified the need for actions to mitigate risks concerning the lack of IoT privacy standards. Current legislative actions show a trend toward consumer IoT devices. Only recently, this focus shifted also to government IoT, smart cities, and critical infrastructures, like power plants, transportation, or the health system [111].

Despite the imminent threat posed by unregulated and insecure IoT devices, many countries are reluctant to create new regulations to hinder innovation and economic growth. A harmonized movement around the globe could break up such motives [111]. If every manufacturer had to comply with the same standard security and privacy rules, no country would suffer from IoT-based disadvantages. Furthermore, regarding the mobile nature of IoT devices, it would be highly reasonable to secure, for instance, Swiss IoT devices in the same way as IoT devices placed a few miles North, e.g., on German soil.

9.5. Forensics

IoT Forensics [113] can be recognized as a subset of Digital Forensics (DF). While DF has a long history, IoT Forensics is a

relatively young field. The goal of IoT Forensics is to discover and extract digital information in a legal and forensically sound manner, similar to the goal of DF. In IoT, forensic data can be acquired via the IoT device itself, the network, or the cloud, which is referred to as the 1-2-3-Zone Approach [114].

However, there exist differences between IoT and security and forensics. Typically, IoT security protects against both physical and logical security threats. It uses a variety of security methods to reduce the attack's scope and prevent further damage, providing a real-time response, *i.e.*, employing a variety of approaches to combat threats amid a life crisis. Considering the scope, security broadens the scope, searching for any potentially dangerous activity 24 h a day, seven days a week by implementing a set of security procedures, processes, and standards to create a safe system and prevent future cyber-threats.

IoT forensics analyzes physical evidence and electronic data to determine and reconstruct the chain of events by preserving and analyzing digital information using investigative approaches. Forensics focuses on postmortem investigations, *i.e.*, finding deficiencies after the incident or when the system is dormant, however, forensics professionals might capture digital evidence during a real-time incident, when using live forensics techniques. Considering the scope, forensics is case-related, re-enacting a specific criminal scenario. Forensics satisfies requirements and follows standards to be prepared to conduct an investigation. Forensics takes measurements to maximize the forensic value of prospective evidence, while reducing the amount of resources spent on the investigation. So far, several theoretical frameworks were already established to deal with forensics in the IoT realm, such as the 3D framework [115], the Next-Best-Thing Triage Model [114], or the Forensics-Aware Model for the IoT [116].

Research recommends two possible options for existing digital forensics tools and methodologies [113]. While some authors [117,118] provide holistic frameworks meant to be applicable across the forensic spectrum, others criticize this approach as too broad, preferring to focus on specific use cases, such as a forensic framework for a particular environment [119,120].

9.6. Life-cycle management

Special care and advanced methodologies need to be applied in any step of the life cycle of a secure node, *i.e.*, bootstrapping, commissioning, operation, upgrade, or decommissioning [121]. IoT environments are built by heterogeneous smart devices produced by a variety of manufacturers and characterized by very diverse resources and constraints. The bootstrapping process covers the process that allows an embedded device to join and operate in the network. Many secure bootstrapping protocols rely on pre-shared authentication keys (or attestation tokens) supported by a third party (running either online or offline) [122]. Such an approach turns out to be not flexible enough in many resource-constrained environments due to the complexity of this additional entity. Furthermore, this overcomplicates the runtime assurance of deployed edge devices, since possible software and firmware updates need to be vendor-specific, thus, limiting the vision toward a generic third party solution. Finally, when the device is unable to maintain a high level of security anymore, decommissioning of the device has to be executed.

9.7. Ongoing projects and existing guidelines

The products selected and outlined above were built to protect vulnerable IoT devices. However, they do not solve all problems of IoT devices. While a “symptom control” is possible, products must be designed to be safe from the start. For this reason, one dedicated IoT project implementing secure access and network functionality (*cf.* Section 9.7.1) and another one with IoT guidelines

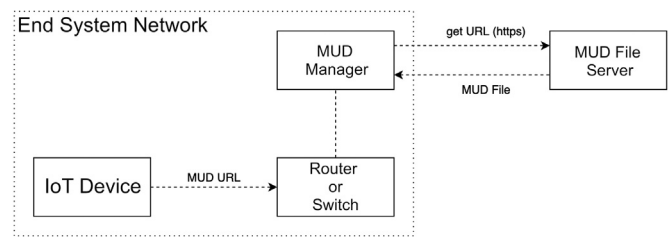


Fig. 4. Manufacturer usage description architecture based on [129].

for manufacturers, containing best practices for design, development, and deployment of secure IoT services and products (*cf.* Section 9.7.2), are selected for a detailed description here. More generally, other related projects and guidelines in this context to be mentioned are the Broadband Internet Technical Advisory Group (BITAG) [123], the Cloud Security Alliance (CSA) [124], and projects by OWASP [69]. Even governmental institutions, such as the National Institute of Standards and Technology (NIST) [125], Homeland Security [126], or transnational agencies, like the European Union Agency for Cybersecurity (ENISA) [127], provide as of now newer guidelines and respective discussions.

9.7.1. IETF

The Internet Engineering Task Force (IETF) encompasses “a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet” [128]. In order to reduce the attack surface of the communication of IoT devices, the IETF developed the *Manufacturer Usage Description* (MUD). MUD is concerned with the creation of network access control policies. As a result, such rules may be easily imposed using the Software-Defined Networking (SDN) paradigm. However, beyond network-level aspects, the MUD semantics do not allow for the definition of security properties, which would allow for a more fine-grained approach to determining how IoT devices should communicate. MUD is based on the principle that each IoT device, *e.g.*, a light bulb, has a dedicated and specific purpose. Therefore, all other use cases are not “acceptable”.

Consequently, a MUD can be formulated for the example of the light bulb: it has to be controlled remotely via the network and may offer a connection to a rendezvous service to enable its detection by a smartphone app. The MUD defines that the light bulb only talks to that one rendezvous service, but not to other devices or services [129]. This ensures that the light bulb is only used for the intended purpose.

The MUD and its architecture are depicted in Fig. 4 for which the MUD Uniform Resource Locator (URL) is a URL stored on the IoT device pointing to the MUD file server (usually provided by the manufacturer) from which the MUD can be downloaded.

The MUD URL is sent from the device (Thing) to a router or switch for accessing a MUD file. This is usually embedded in the Dynamic Host Configuration Protocol (DHCP) request. The router passes the MUD URL to the MUD manager, which downloads the MUD file from the manufacturer's server (MUD file server). Finally, the MUD Manager is responsible for ensuring that these specifications within the MUD file are implemented in the network.

Two components are essentially necessary for the network to ensure the functionality of the MUD specification, which may be considered as a drawback. Not only the manufacturer of the IoT device itself needs to comply with the specification, but (a) also switches and routers in the network have to implement the MUD protocol and (b) at least one MUD manager service must be

operational. However, networking companies already announced in 2019 to provide MUD support in their enterprise network solutions [130].

9.7.2. GSMA

The Global System for Mobile Communications Association (GSMA) “represents the interests of mobile operators worldwide, uniting more than 750 operators with almost 400 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organizations in adjacent industry sectors” [131]. Consequently, their recommendation *GSMA IoT Security Guidelines* provides detailed recommendations for the secure design, development, and deployment of IoT services, networks, and endpoints. Also, several attack scenarios are included to show manufacturers, how their products could be compromised and how these scenarios can be prevented with standard best practices. Furthermore, the guideline provides a security assessment framework, which manufacturers can use to test their products. If manufacturers do not have sufficient resources or expertise, there also exists the option of assessment of a service, whereby an external company goes through the assessment framework and tests the IoT solution under investigations [132].

9.8. New products for increased IoT security

An overview of software-related as well as hard- and firmware-related discusses the state-of-the-art.

9.8.1. Software

Products, where security is mainly achieved through a software component, fall into this category. More precisely, security logic is added by running software on the same network as these IoT devices operate in. Here, Intrusion Detection Systems (IDS) act as an additional line of defense by detecting attackers. Namely, they monitor activities of a host or network and can trigger alerts or launch mitigation actions when unusual behavior is detected [72]. However, creating an IDS that functions with maximum accuracy and minimal false alerts is a challenging task [133]. Thus, two selected examples of such software solutions are analyzed here.

Armis security. Armis offers an agentless security platform for businesses. The product integrates into the customer's existing infrastructure with no additional hardware. The system typically runs in a virtual machine and can be installed on any existing server within the network to be monitored. The network does not need to scan for devices actively, but traffic is passively analyzed. By querying the device knowledge base, it can identify and classify every device on the network, whether managed or unmanaged. The database contains profiles and properties of devices. Based on this information, the security platform can assess the risk for each device. For example, it knows if the device is running an old operating system version. In addition, the behavior can be compared to the behavioral data stored in the knowledge base. If anomalies are detected, a warning can be issued. Not only detection is possible, but automated response actions can also be implemented. Armis integrates with network access control products from networking companies like Cisco. As a threat response measure, Armis can trigger a quarantine on a suspicious or malicious device [134].

The Armis security platform is classified as an IDS. It is only installed conveniently on a single device in the network. However, it can be challenging to detect an attack if it runs in a separate part of the network [72]. Generally, Armis compares network behavior with known attack signatures or patterns and compares a node's behavior with the expected behavior based on historical data. Following the IDS placement strategies and threat detection methods defined by [72], Armis uses a centralized placement strategy and a hybrid threat detection method.

Bastille. Bastille is another software solution, which allows for the monitoring of a specific area, for example, an entire office, for the presence and behavior of connected devices, which use cellular (cell phones), WiFi, Bluetooth, or Bluetooth Low Energy (BLE) radio signals. Although the approach is categorized as “software”, hardware sensors are also needed for its operation. The approach is based on the three pillars *Discover*, *Analyze*, and *Act*. Bastille scans the room and *discovers* wireless transmitters. By digitally demodulating radio signals, protocols can be identified, and individual devices can be plotted on a map of the room, even showing their position. Those devices found are *analyzed* for protocols, traffic, and other devices connected to them. This can then be used to decide whether a device is under attack or performs a prohibited action. An example of a non-permitted action would be when a hearing aid establishes a connection to a device outside the monitored area, allowing an attacker to listen to what is communicated inside the office. When such a treat is detected, different *actions* can be taken. If a device is detected, which is prohibited in that area or exhibits abnormal behavior, it can either be physically removed or isolated [135].

This solution is mainly used to detect devices. Therefore, the IDS focuses on the physical intrusion of devices into a monitored space. An advantage is that devices not part of a specific network are also recognized. All devices that are located within the room monitored by sensors are discovered and surveyed. However, the system's capabilities are more limited with respect to detecting unusual behavior.

9.8.2. Hardware and firmware

To secure resource-limited IoT devices without the need to install additional software, products in the category *Hardware and Firmware* can be used. The following ones determine selected examples.

ReFirm labs. Every IoT device runs firmware in control of the hardware. If a firmware exposes vulnerabilities, such as weak passwords, backdoors, outdated components, or zero-day vulnerabilities, these can be exploited by an attacker. ReFirm Labs' tool can automatically analyze firmware, intended to be used by manufacturers of IoT products or to check devices installed from other manufacturers on their security level. The Centrifuge Platform takes a firmware's binary image as input and the output generated contains a detailed security audit. Based on the information available, manufacturers' own developers can take corrective actions to the firmware or, if a third party supplies the device, they can be informed about possible attack vectors in their products [136].

ReFirm labs' solution addresses security problems faced by manufacturers. This is especially valuable, because it hardens the security of IoT products already in the development process. While this strengthens the pre-deployment phase, this can also be seen as a limitation, since manufacturers and IT experts can only use this approach to secure the products developed.

Zymbit. It offers an HSM *Zymkey*, which is a plug-in hardware module for the Raspberry Pi [137]. It supports the security goals of authentication and integrity. The module can be plugged into a Raspberry Pi and is controlled via an API, which covers the creation and storing of a unique device ID in the hardware module, containing a solid cryptographic engine, storing public/private key pairs that cannot leave the module, and offering a physical tamper detection, such as an accelerometer detecting vibrations and orientation change events [138]. An advantage of this approach is the simple integration with a Raspberry Pi. However, this dedicated hardware dependency determines a general drawback, too.

9.8.3. Service and cloud

Cloud computing is an increasingly important topic due to the reduction of fixed-costs, e.g., by eliminating the need to purchase hardware, excellent scalability characteristics, and approximately 24/7 availability. IoT systems and their security shall be considered in the same line. And since many technology companies, such as Amazon [139], Google [140], Microsoft [141], IBM [142], offer competitive products, but the basics of these systems are comparable, only Amazon's system is covered.

Amazon. The development of an entire ecosystem of IoT services in the Amazon Web Services (AWS) Cloud ensures the security of a fleet of distributed devices, since Amazon offers a dedicated "AWS IoT Device Defender" service. Two main features can be highlighted. The service continuously checks the configuration of all connected IoT devices and checks, whether predefined best practices are respected. An example is whether all devices operate on valid X.509 certificates, e.g., based on TLS or Secure Sockets Layer (SSL). Secondly, it is possible to detect unusual behavior on devices. Predefined rules determine the expected behavior, e.g., restricting entities the device is allowed to connect or limiting how much data is received or sent. Based on these rules, alerts will be generated [139].

A cloud service has the advantage of minimal setup effort for an already existing network. However, a limitation of Amazon's solution is that the value of their service can only be fully realized, if other services from AWS are consumed. For example, it is also recommended to use the services "AWS IoT Core", "AWS IoT Device Management", "AWS IoT Analytics". This creates a vendor lock-in effect, making it challenging to switch to another provider.

9.8.4. Home use

With the increasing introduction of connected and intelligent devices in households, cyberattacks in the private sphere also increase. Products like Bitdefender BOX try to remedy this threat.

Bitdefender. Bitdefender advertises BOX as an-all-in one product for a secure, connected home. It can act as a standalone WiFi router or be connected to an existing one. By constantly scanning all traffic and using machine learning to process the data, the system learns about the expected behavior of devices and can detect anomalies [143]. This product can be compared to the industrial Armis security solution, since it is categorized as a centralized IDS. The detection method runs an anomaly-based approach, based on [72]. It uses historical data to learn about expected behavior to detect unusual behavior.

9.9. IoT business outlook

Although the discussion and definition of IoT security as above revealed that their importance is crucial, but not always IoT devices meet such technical and regulative requirements, a brief IoT security market analysis depicts market forces in terms of historical growth and estimations of their future trajectory.

The market for IoT devices is growing steadily. As outlined in Section 3 an estimated 31 billion IoT devices online (2020) are expected to grow to as many as 75 billion by 2025 [13]. The enormous growth is also reflected in the market sizes (cf. Fig. 5). The consumer's Smart Home and the industrial market belong to the five biggest IoT sectors next to Smart Cities, Connected Health, and Connected Cars. This is why those two markets were chosen as indicators for the IoT security market [146]. From 2017 to 2025, the market size in the industrial IoT segment alone is expected to rise from 61.8 billion \$US to 110.6 billion \$US, corresponding to growth by a factor of nearly two. Similarly, rapid growth can also be observed in the Smart Home market segment. Here, 83 billion

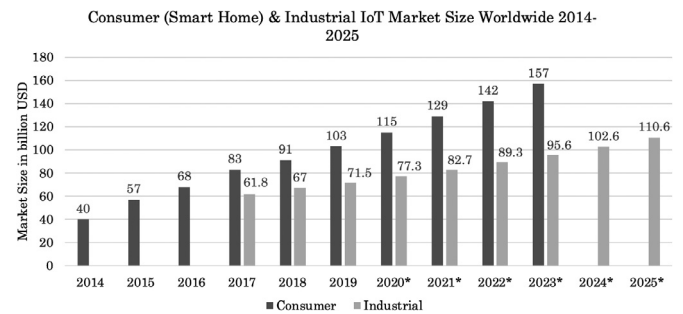


Fig. 5. 2014 to 2025 consumer smart home and industrial IoT market size based on [144,145] (* = Forecasts).

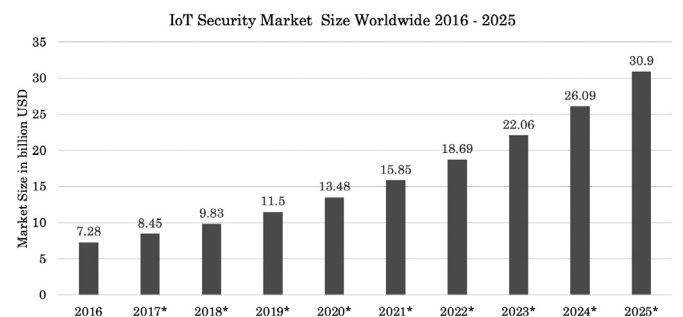


Fig. 6. 2016 to 2025 IoT security market size based on [147] (* = Forecasts).

\$US were spent in 2017 and is expected to grow to 157 billion \$US by 2023. This again represents almost a doubling of volume compared to the industrial market in an even shorter time.

As discussed in Section 7, many IoT systems still see room for improvements in terms of security. A hasty market launch of IoT products may have contributed to this fact, but business opportunities arise from such new challenges, too. The market study [148] estimates the market capitalization for IoT security at 12.5 billion \$US in 2020, and they expect it to rise to 36.6 billion \$US by 2025. That would be more than doubling the size in 5 years. Another market estimate from 2017 painted a similar picture (cf. Fig. 6). It predicted market size of 13.48 billion \$US in 2020 and a growth of 30.9 billion \$US by 2025. Comparing these numbers with the growth of the industrial and Smart Home IoT sectors reflects the delayed response on the security side.

10. Discussion

Considering the vast numbers of IoT devices currently being deployed and the number of devices that are estimated to exist in 2025, it is indisputable that IoT will have a significant impact on the society and economy [13]. IoT devices rapidly did become part of everyday life [71] and all relevant sectors will encounter them. As pointed out by [16], selected industries are already fully involved in the development of IoT applications: factories, medical institutions, homes, and cities.

Due to this growth and entanglement into every day's life, IoT failures and attacks can be severe. Hence, IoT security is a concern of extreme significance. [53] examined research projects from 2016 to 2018 and infers that several challenges in securing IoT devices and networks exist. Due to the particular characteristics of IoT devices, it is not feasible to apply traditional IT countermeasures, since only dedicated IoT security procedures

have to be developed [3,53,63,65,70,71]. However, since there is already considerable progress made in relevant fields, especially IoT device hardware, network management, authentication, privacy policies, forensics, and life-cycle management, the path to secure IoT has been opened.

Already [53] concludes that the fast progress of IoT security research identified can be supported by various products emerging on the market. While products can be distinguished as *Software*, *Hardware/ Firmware*, *Service/Cloud*, and *Home* solutions, depending on where security measures are applied to, for software solutions the most common approach still refers to Intrusion Detection Systems [72]. Hardware and firmware solutions secure IoT devices without installing additional software and are primarily intended for IoT manufacturers [136]. Service and cloud products focus on securing the entire network of distributed IoT devices by checking their configuration and monitoring their behavior to detect unusual actions [139]. In private households, the key objective of IoT security is to protect the users' privacy [143]. Home solutions can scan data traffic and ensure that no sensitive information is leaked.

Within the same context, the need for regulations arose. Multiple projects and working groups, such as IETF, GSMA, OWASP, or BITAG, elaborate best practices for the design, development, and deployment of secure IoT services and products. This shared knowledge makes it possible for smaller manufacturers with smaller expertise and limited resources to offer secure IoT ecosystems. Furthermore, governmental agencies, like the American Homeland Security, National Institute of Standards and Technology (NIST), or the European ENISA, work on regulations or guidelines to protect the population. However, several gaps between existing regulations like GDPR and the IoT domain remain still unsettled.

The threat taxonomy developed here and based on the literature reviews (cf. Section 8.2) provides a more exhaustive view of possible IoT threats and IoT attack vectors than existing taxonomies do. However, while the taxonomy is based on the three-layer IoT architecture, the categorization based on layers helps to visualize where a threat can occur, which is limited due to its simplicity. For selected threats, it is not trivial where they should be positioned within the taxonomy. For example, a DDoS threat can affect the network and the application layer. Additionally, the taxonomy does not address that selected threats differing in nature depending on the context: a node within the system can be on the receiving end of a DDoS attack, i.e., if other nodes are sending requests to it, or on the sending end, i.e., if it was compromised and sends requests to other nodes.

Additionally, [65] highlights the importance of considering the complete lifecycle of IoT devices when addressing security concerns. However, the taxonomy presented does not account for the dynamic nature of IoT systems, where devices might join a network at any time and devices might belong to multiple owners during their life-cycle. Thus, such a false impression of addressing IoT security as a single task has to be countermeasured, since securing the system needs to be a permanent task.

Future versions of this taxonomy can address these aspects by incorporating a dynamic view of IoT security. Additionally, they can include a ranking of threats based on metrics, such as the Common Vulnerability Scoring System (CVSS) by NIST [149]. By adding data from public data sets, such as the Common Vulnerabilities and Exposure (CVE) database [150], which lists known vulnerabilities, an additional perspective can be determined on how common specific threats are. It will be interesting to explore how these threats can be combined to form common attack paths that a malicious user might take.

11. Summary and conclusions

While the market of IoT in general grows at a strong pace, the market for IoT security is still in its infancy. Vulnerabilities of IoT devices have been and will be exploited in cyberattacks. The Mirai Botnet or the computer worm Stuxnet will not be the last ones of their kind. However, recognizing threats posed by insecure IoT devices, their use in dedicated scenarios, and identifying the need for basic (or additional) security measures are the first step in the right direction.

For the development of IoT security measures, it is essential to question why it is technically challenging to secure IoT devices. The analysis of particular characteristics of IoT devices revealed clearly that features like usability, limited resources, ubiquity, short time-to-market, and interconnectivity prove that traditional security measures cannot be applied one-to-one. Dedicated models and, in turn, products are needed to secure the IoT domain. The list of IoT security objectives compiled, and the threat taxonomy developed can serve as a guideline for manufacturers to specify, design, and implement secure devices and to decrease the number of attack vectors an adversary can potentially use to target an attack. Gratifyingly, as Section 9 outlines, several promising technologies and products on the market exist, which can make the use of IoT technology secure. In addition to these products available, institutions and working groups unite their forces and knowledge to formulate guidelines such that manufacturers can build secure IoT devices in the first place. However, there is room for additional security products and services as the markets' growth trajectories demand.

To conclude, the security landscape of IoT is on the move and in the right direction. Nevertheless, it needs to enhance its speed, since many IoT devices and potential threats increase exponentially. Secure products, well-aligned to determine security requirements stated in detail, are to be developed by manufacturers soon. More affordable security measures need to be offered and tailored to resource-constrained IoT devices. Consumers will have to be responsible and security-aware, supported by regulations, guidelines, and governments that pay attention to this market at a sufficient level. Consumers as well as manufacturers and governments have to take on their role to exploit the power and innovation IoT offers, but need to make the world a safer place at the same time, too.

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

This paper was supported partially by (a) the University of Zürich UZH, Switzerland, and (b) the European Union's Horizon 2020 Research and Innovation Program under Grant Agreement No. 830927, the CONCORDIA project.

References

- [1] K. Schwab, The fourth industrial revolution: What it means, how to respond, 2016, Accessed: 2020-11-11. [Online]. Available: <https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/>.
- [2] Q. Gou, L. Yan, Y. Liu, Y. Li, Construction and strategies in IoT security system, in: *International Conference on Green Computing and Communications and Internet of Things and Cyber, Physical and Social Computing*, IEEE, Piscataway, NJ, US, 2013, pp. 1129–1132.

- [3] J. Pacheco, D. Ibarra, A. Vijay, S. Hariri, IoT security framework for smart water system, in: IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA), IEEE, Piscataway, NJ, US, 2017, pp. 1285–1292.
- [4] M. Vega, Internet of things statistics, facts & predictions (2020's update), 2020, Accessed: 2020-10-17. [Online]. Available: <https://review42.com/internet-of-things-stats/>.
- [5] G.D. Maayan, The IoT rundown for 2020: Stats, risks, and solutions, 2020, Accessed: 2020-11-12. [Online]. Available: <https://securitytoday.com/Articles/2020/01/13/The-IoT-Rundown-for-2020.aspx?Page=1&p=1>.
- [6] R. van der Meulen, Gartner says 8.4 billion connected "Things" will be in use in 2017, up 31 percent from 2016, 2017, Accessed: 2020-10-17. [Online]. Available: <https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016>.
- [7] S. Liu, Internet of things (IoT) - Statistics & facts, 2020, Accessed: 2020-11-09. [Online]. Available: <https://www.statista.com/topics/2637/internet-of-things/>.
- [8] S. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-Porisini, Security, privacy and trust in internet of things: The road ahead, Elsevier Comput. Netw. 76 (2015) 146–164.
- [9] J. Romkey, Toast of the IoT: The 1990 interop internet toaster, IEEE Consum. Electron. Mag. 6 (1) (2017) 116–119.
- [10] V. Rajaraman, Radio frequency identification, Resonance 22 (6) (2017) 549–575.
- [11] P. Suresh, J.V. Daniel, V. Parthasarathy, R.H. Aswathy, A state of the art review on the internet of things (IoT) history, technology and fields of deployment, in: International Conference on Science Engineering and Management Research (ICSEMR), IEEE, Piscataway, NJ, US, 2014, pp. 1–8.
- [12] C.T. Mark Patel, What's new with the internet of things?, 2017, Accessed: 2020-11-12. [Online]. Available: <https://www.mckinsey.com/industries/semiconductors/our-insights/whats-new-with-the-internet-of-things#>.
- [13] Cisco Systems Inc., Cisco annual internet report (2018–2023), 2020, Accessed: 2020-11-11. [Online]. Available: <https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf>.
- [14] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, M. Gidlund, Industrial internet of things: Challenges, opportunities, and directions, IEEE Trans. Ind. Inf. 14 (11) (2018) 4724–4734.
- [15] A. Gatouillat, Y. Badr, B. Massot, E. Sejdić, Internet of medical things: A review of recent contributions dealing with cyber-physical systems in medicine, IEEE Internet Things J. 5 (5) (2018) 3810–3822.
- [16] Congressional Research Service, The internet of things (IoT): An overview, 2020, Accessed: 2020-11-12. [Online]. Available: <https://fas.org/spp/crs/misc/IF11239.pdf>.
- [17] S. Mukherjee, S. Patel, S. Kales, N. Ayas, K. Strohl, D. Gozal, A. Malhotra, An official American thoracic society statement: The importance of healthy sleep, ATS J. Am. J. Respir. Crit. Care Med. 191 (12) (2015) 1450–1458.
- [18] J. Tsai, E.S. Ford, C. Li, G. Zhao, L.S. Balluz, Physical activity and optimal self-rated health of adults with and without diabetes, BMC Public Health 10 (2010) 365.
- [19] R. Bharadwaj, The state of IoT in insurance – Automotive, home, and health, 2019, Accessed: 2020-11-12. [Online]. Available: <https://emerj.com/partner-content/iot-insurance-automotive-home-health/>.
- [20] H. Arasteh, V. Hosseinneshad, V. Loia, A. Tommasetti, O. Troisi, M. Shafie-khah, P. Siano, IoT-based smart cities: A survey, in: 2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC), 2016, pp. 1–6.
- [21] L. Horwitz, Can smart city infrastructure alleviate the strain of city growth?, 2020, Accessed: 2020-11-12. [Online]. Available: <https://www.cisco.com/c/en/us/solutions/internet-of-things/smart-city-infrastructure.html>.
- [22] J. Manyika, et al., Open data: Unlocking innovation and performance with liquid information, 2013, Accessed: 2020-11-12. [Online]. Available: <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/open-data-unlocking-innovation-and-performance-with-liquid-information>.
- [23] M. Alaa, A.A. Zaidan, B.B. Zaidan, M. Talal, M.L.M. Kiah, A review of smart home applications based on Internet of Things, J. Netw. Comput. Appl. 97 (2017) 48–65.
- [24] V. Voydock, S. Kent, Security mechanisms in high-level network protocols, ACM Comput. Surv. 15 (2) (1983) 135–171.
- [25] H. Federrath, A. Pfizmann, Gliederung und systematisierung von schutzzielen in IT-systemen, Springer Datenschutz Datensicherheit (DuD) 24 (12) (2000) 704–710.
- [26] K.C. Laudon, J.P. Laudon, D. Schoder, Wirtschaftsinformatik, Pearson Deutschland, Hallbergmoos, Germany, 2015.
- [27] Q. Do, B. Martini, K.-K.R. Choo, The role of the adversary model in applied security research, Comput. Secur. 81 (2019) 156–181, [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0167404818306369>.
- [28] Q.-D. Ngo, H.-T. Nguyen, V.-H. Le, D.-H. Nguyen, A survey of IoT malware and detection methods based on static features, ICT Express 6 (4) (2020) 280–286, [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2405959520300503>.
- [29] R. Shirley, Internet security glossary, 2000, Accessed: 2020-10-22. [Online]. Available: <https://www.rfc-editor.org/rfc/pdf/rfc2828.txt.pdf>.
- [30] D. Evans, G. Jarboe, H. Thomases, M. Smith, C. Treadaway, Networking Complete, third ed., Wiley, New York, NY, US, 2002.
- [31] T.J. Grant, R.H.P. Janssen, H. Monsuur, Network Topology in Command and Control: Organization, Operation, and Evolution, IGI Global, 2014.
- [32] Cisco Systems Inc., What is network topology?, 2020, Accessed: 2020-10-26. [Online]. Available: <https://www.cisco.com/c/en/us/solutions/automation/network-topology.html>.
- [33] A. Cilfone, L. Davoli, L. Belli, G. Ferrari, Wireless mesh networking: An IoT-oriented perspective survey on relevant technologies, MDPI Future Internet 11 (4) (2019) 99.
- [34] A.T.-Y. Lin, J. Lee, D. Lee, C.-C. Chen, The development of IC packaging under the Internet of Things standards, in: 2016 11th International Microsystems, Packaging, Assembly and Circuits Technology Conference (IMPACT), 2016, pp. 209–211.
- [35] S. Devalal, A. Karthikeyan, LoRa technology - An overview, in: 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), 2018, pp. 284–290.
- [36] C. Ebi, F. Schaltegger, A. Rüst, F. Blumensaat, Synchronous LoRa mesh network to monitor processes in underground infrastructure, IEEE Access 7 (2019) 57663–57677.
- [37] B. Stiller, E. Schiller, C. Schmitt, An overview of network communication technologies for IoT, in: Handbook of Internet-of-Things, Springer, Cham, Switzerland, 2021, ch. 12.
- [38] Z. Shelby, C. Bormann, 6LoWPAN - the Wireless Embedded Internet, Wiley-Blackwell, West Sussex, England, UK, 2009.
- [39] N. Kushalnagar, G. Montenegro, C. Schumacher, IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals, RFC 4919 (Informational), RFC Editor, Fremont, CA, USA, 2007, pp. 1–12, [Online]. Available: <https://www.rfc-editor.org/rfc/rfc4919.txt>.
- [40] E. Kim, D. Kaspar, C. Gomez, C. Bormann, Problem Statement and Requirements for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing, RFC 6606 (Informational), RFC Editor, Fremont, CA, USA, 2012, pp. 1–32, [Online]. Available: <https://www.rfc-editor.org/rfc/rfc6606.txt>.
- [41] Z. Shelby, S. Chakrabarti, E. Nordmark, C. Bormann, Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs), RFC 6775 (Proposed Standard), RFC Editor, Fremont, CA, USA, 2012, pp. 1–55, [Online]. Available: <https://www.rfc-editor.org/rfc/rfc6775.txt>.
- [42] S. Chakrabarti, G. Montenegro, R. Droms, J. Woodyatt, IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) ESC Dispatch Code Points and Guidelines, RFC 8066 (Proposed Standard), RFC Editor, Fremont, CA, USA, 2017, pp. 1–9, [Online]. Available: <https://www.rfc-editor.org/rfc/rfc8066.txt>.
- [43] P. Thubert, R. Cragie, IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Paging Dispatch, RFC 8025 (Proposed Standard), RFC Editor, Fremont, CA, USA, 2016, pp. 1–8, [Online]. Available: <https://www.rfc-editor.org/rfc/rfc8025.txt>.
- [44] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, G. Carle, DTLS based security and two-way authentication for the Internet of Things, Ad Hoc Netw. 11 (8) (2013) 2710–2723.
- [45] Berkeley WEBS, Project Page for blip, the Berkeley IP implementation for low-power networks, 2011, last access: April 20, 2020. [Online]. Available: <http://tinyurl.com/bliptutorial>.
- [46] C. Bormann, A.P. Castellani, Z. Shelby, CoAP: An application protocol for billions of tiny internet nodes, IEEE Internet Comput. 16 (2) (2012) 62–67.
- [47] M.B. Tamboli, D. Dambawade, Secure and efficient CoAP based authentication and access control for Internet of Things (IoT), in: 2016 IEEE International Conference on Recent Trends in Electronics, Information Communication Technology (RTEICT), 2016, pp. 1245–1250.
- [48] S. Arvind, V.A. Narayanan, An overview of security in CoAP: Attack and analysis, in: 2019 5th International Conference on Advanced Computing Communication Systems (ICACCS), 2019, pp. 655–660.
- [49] M.B. Yassein, M.Q. Shatnawi, D. Al-zoubi, Application layer protocols for the Internet of Things: A survey, in: 2016 International Conference on Engineering MIS (ICEMIS), 2016, pp. 1–4.
- [50] G. Suciu, C.-I. Istrate, M.-C. Diță, Secure smart agriculture monitoring technique through isolation, in: 2019 Global IoT Summit (GloTS), 2019, pp. 1–5.
- [51] S. Li, Security architecture in the internet of things, in: Securing the Internet of Things, IEEE, Piscataway, NJ, US, 2017, pp. 27–48, ch. 2.
- [52] P. Sethi, S.R. Sarangi, Internet of things: Architectures, protocols, and applications, Hindawi J. Electr. Comput. Eng. 2017 (2017).

- [53] M.B.M. Noor, W.H. Hassan, Current research on internet of things (IoT) security: A survey, *Elsevier Comput. Netw.* 148 (2019) 283–294, Accessed: 2020-12-02. [Online]. Available: <https://doi.org/10.1016/j.comnet.2018.11.025>.
- [54] A. Bujari, M. Furini, F. Mandreoli, R. Martoglia, M. Montanero, D. Ronzani, Standards, security and business models: Key challenges for the IoT scenario, *Mob. Netw. Appl.* 23 (1) (2018) 147–154, [Online]. Available: <https://doi.org/10.1007/s11036-017-0835-8>.
- [55] J. Zhang, H. Chen, L. Gong, J. Cao, Z. Gu, The current research of IoT security, in: 4th International Conference on Data Science in Cyberspace (DSC), IEEE, Piscataway, NJ, US, 2019, pp. 346–353.
- [56] W. Stallings, The internet of things: Network and security architecture, *Internet Soc.: Internet Protocol J.* 18 (4) (2015) 2–24.
- [57] P.Y. Zhang, M.C. Zhou, G. Fortino, Security and trust issues in fog computing: A survey, *Elsevier Future Gener. Comput. Syst.* 88 (2018) 16–27, [Online]. Available: <https://doi.org/10.1016/j.future.2018.05.008>.
- [58] C. Koliass, G. Kambourakis, A. Stavrou, J. Voas, DDos in the IoT: Mirai and other botnets, *IEEE Comput.* 50 (7) (2017) 80–84.
- [59] Oracle, Oracle DNS, 2021, Accessed: 2021-04-21. [Online]. Available: <https://www.oracle.com/corporate/acquisitions/dyn>.
- [60] M.R. Jordan Robertson, Cybersecurity – Mysterious '08 Turkey pipeline blast opened new cyberwar, 2014, Accessed: 2020-12-09. [Online]. Available: <https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar>.
- [61] T. Stevens, Cyberweapons: Power and the governance of the invisible, *Springer Int. Politics* 55 (3–4) (2018) 482–502.
- [62] S. Singh, N. Singh, Internet of things (IoT): Security challenges, business opportunities & reference architecture for E-commerce, in: International Conference on Green Computing and Internet of Things (ICGCIOT), IEEE, Piscataway, NJ, US, 2015, pp. 1577–1581.
- [63] C. Koliass, A. Stavrou, J. Voas, Securely making things right, *IEEE Comput.* 48 (9) (2015) 84–88.
- [64] S. Babar, P. Mahalle, A. Stango, N. Prasad, R. Prasad, Proposed security model and threat taxonomy for the internet of things (IoT), in: International Conference on Network Security and Applications, Springer, Cham, Switzerland, 2010, pp. 420–429.
- [65] O. Garcia-Morcho, S. Kumar, M. Sethi, Internet of Things (IoT) Security: State of the Art and Challenges, Internet Research Task Force (IRTF), no. 8576, 2019, pp. 1–50, [Online]. Available: <https://rfc-editor.org/rfc/rfc8576.txt>.
- [66] D. Bastos, F. Giubilo, M. Shackleton, F. El-Moussa, GDPR privacy implications for the internet of things, in: 4th Annual IoT Security Foundation Conference, London, UK, 2018.
- [67] Ponemon, Ponemon institute, 2020, Accessed: 2020-11-12. [Online]. Available: <https://www.ponemon.org/>.
- [68] M. Drolet, What does stolen data cost [per second], 2018, Accessed: 2020-10-28. [Online]. Available: <https://www.csoonline.com/article/3251606/what-does-stolen-data-cost-per-second.html>.
- [69] OWASP, OWASP internet of things project, 2018, Accessed: 2020-12-16. [Online]. Available: https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=Main.
- [70] S. Notra, M. Siddiqi, H.H. Gharakheili, V. Sivaraman, R. Boreli, An experimental study of security and privacy risks with emerging household appliances, in: Conference on Communications and Network Security, IEEE, Piscataway, NJ, US, 2014, pp. 79–84.
- [71] D. Minoli, K. Sohraby, J. Kouns, IoT security (IoTsec) considerations, requirements, and architectures, in: 14th Annual Consumer Communications & Networking Conference (CCNC), IEEE, Piscataway, NJ, US, 2017, pp. 1006–1007.
- [72] B.B. Zarpelão, R.S. Miani, C.T. Kawakani, S.C. de Alvarenga, A survey of intrusion detection in internet of things, *Elsevier J. Netw. Comput. Appl.* 84 (2017) 25–37.
- [73] G. Jonsdottir, D. Wood, R. Doshi, IoT network monitor, in: 2017 MIT Undergraduate Research Technology Conference (URTC), IEEE, Piscataway, NJ, US, 2017, pp. 1–5.
- [74] S. Nam, S. Jeon, H. Kim, J. Moon, Recurrent gans password cracker for iot password security enhancement, *Sensors* 20 (11) (2020) 3106.
- [75] H. Hellaoui, M. Koudil, A. Bouabdallah, Energy-efficient mechanisms in security of the internet of things: A survey, *Elsevier Comput. Netw.* 127 (2017) 173–189.
- [76] C. Bormann, M. Ersue, A. Keranen, Terminology for Constrained-Node Networks, Internet Engineering Task Force (IETF), Fremont, CA, USA, (ISSN: 2070-1721) 2014, pp. 1–17, Accessed: 2020-12-07. [Online]. Available: <https://www.hjrp.at/doc/rfc/rfc7228.html>.
- [77] A.K. Das, S. Zeadally, D. He, Taxonomy and analysis of security protocols for internet of things, *Elsevier Future Gener. Comput. Syst.* 89 (2018) 110–125, [Online]. Available: <https://doi.org/10.1016/j.future.2018.06.027>.
- [78] I. Alqassem, D. Svetinovic, A taxonomy of security and privacy requirements for the internet of things (IoT), in: International Conference on Industrial Engineering and Engineering Management, IEEE, Piscataway, NJ, US, 2014, pp. 1244–1248.
- [79] R. Roman, J. Zhou, J. Lopez, On the features and challenges of security and privacy in distributed internet of things, *Elsevier Comput. Netw.* 57 (10) (2013) 2266–2279, [Online]. Available: <http://dx.doi.org/10.1016/j.comnet.2012.12.018>.
- [80] S. Tweneboah-Koduah, K.E. Skouby, R. Tadayoni, Cyber security threats to IoT applications and service domains, *Springer Wirel. Personal Commun.* 95 (1) (2017) 169–185.
- [81] M. Nawir, A. Amir, N. Yaakob, O.B. Lynn, Internet of things (IoT): Taxonomy of security attacks, in: 3rd International Conference on Electronic Design, ICED 2016, IEEE, Piscataway, NJ, US, 2016, pp. 321–326.
- [82] J.M. Stewart, Explain the difference between identification and authentication (identity proofing), in: CompTIA Security+™: Review Guide, 2020, Accessed: 2020-12-15. [Online]. Available: https://www.oreilly.com/library/view/comptia-securitytm-review/9780470404843/9780470404843_explain_the_difference_between_identific.html.
- [83] J. Zhou, Z. Cao, X. Dong, A.V. Vasilakos, Security and privacy for cloud-based IoT: Challenges, *IEEE Commun. Mag.* 55 (1) (2017) 26–33.
- [84] T. Martin, D. Geneiatakis, I. Kounelis, S. Kerckhof, I.N. Fovino, Towards a formal IoT security model, *MDPI Symmetry* 12 (8) (2020) 1–16.
- [85] M. El-Hajj, A. Fadlallah, M. Chamoun, A. Serhrouchni, A survey of internet of things (IoT) authentication schemes, *Sensors* 19 (5) (2019) 1141.
- [86] H. Kim, E.A. Lee, Authentication and authorization for the internet of things, *IT Prof.* 19 (5) (2017) 27–33.
- [87] K. Scarfone, J. Wayne, M. Tracy, Confidentiality, integrity, and availability - archive of obsolete content | MDN, in: NIST Special Publication 800-123, Guide To General Server Security, 2018, Accessed: 2020-10-20. [Online]. Available: https://developer.mozilla.org/en-US/docs/Archive/Security/Confidentiality,_Integrity,_and_Availability.
- [88] Y. Lu, L.D. Xu, Internet of things (IoT) cybersecurity research: A review of current research topics, *IEEE Internet Things J.* 6 (2) (2019) 2103–2115.
- [89] Data Privacy Manager, Data privacy vs. data security [definitions and comparisons], 2020, Accessed: 2020-10-20. [Online]. Available: <https://dataprivacymanager.net/security-vs-privacy/>.
- [90] S. Pokorni, Reliability and availability of the internet of things, *Minist. Def. Serb. Armed Forces: Vojnoteh. Glas. / Mil. Tech. Cour.* 67 (3) (2019) 588–600.
- [91] J.A. Onieva, J. Zhou, J. Lopez, Multiparty nonrepudiation: A survey, *ACM Comput. Surv.* 41 (1) (2008).
- [92] J. Pacheco, S. Hariri, IoT security framework for smart cyber infrastructures, in: 1st International Workshops on Foundations and Applications of Self-Systems (FAS-W), IEEE, Piscataway, NJ, US, 2016, pp. 242–247.
- [93] K. Kimani, V. Oduol, K. Langat, Cyber security challenges for IoT-based smart grid networks, *Elsevier Int. J. Crit. Infrastruct. Prot.* 25 (2019) 36–49, [Online]. Available: <https://doi.org/10.1016/j.ijcip.2019.01.001>.
- [94] S. Sidhu, B.J. Mohd, T. Hayajneh, Hardware security in IoT devices with emphasis on hardware Trojans, *J. Sensor Actuator Netw.* 8 (3) (2019) 42.
- [95] T. Schläpfer, A. Rüst, Security on IoT devices with secure elements, in: Embedded World Conference, Nuremberg, Germany, 26–28 Februar 2019, WEKA, 2019.
- [96] S.R. Niya, E. Schiller, I. Cepilov, B. Stiller, BIIT: Standardization of blockchain-based I2ot systems in the I4 era, in: NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium, 2020, pp. 1–9.
- [97] S. Rafati Niya, E. Schiller, B. Stiller, Architectures for blockchain-IoT integration, *Communication Networks and Service Management in the Era of Artificial Intelligence and Machine Learning* (2021) 321–344.
- [98] S. Pinto, N. Santos, Demystifying arm TrustZone: A comprehensive survey, *ACM Comput. Surv.* 51 (6) (2019) [Online]. Available: <https://doi.org/10.1145/3291047>.
- [99] R. Enns, M. Bjorklund, J. Schoenwaelder, A. Bierman, Network configuration protocol (NETCONF), 2011.
- [100] M. Bjorklund, et al., YANG-a data modeling language for the network configuration protocol (NETCONF), 2010.
- [101] R.T. Fielding, Architectural Styles and the Design of Network-Based Software Architectures, University of California, Irvine, 2000.
- [102] J.D.C. Silva, J.J.P.C. Rodrigues, K. Saleem, S.A. Kozlov, R.A.L. Rabêlo, M4DN.IoT-a networks and devices management platform for internet of things, *IEEE Access* 7 (2019) 53305–53313.
- [103] T. Scheffler, O. Bonneß, Manage resource-constrained IoT devices through dynamically generated and deployed YANG models, in: Proceedings of the Applied Networking Research Workshop, 2017, pp. 42–47.
- [104] A. Karim, M.A. Adnan, An OpenID based authentication service mechanisms for internet of things, in: 2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS), 2019, pp. 687–692.
- [105] W. Shang, Y. Yu, R. Droms, L. Zhang, Challenges in IoT networking via TCP/IP architecture, *NDN Proj.* (2016).
- [106] M. Sporny, A. Guy, M. Sabadello, D. Reed, Decentralized identifiers (DIDs) v1.0 core architecture, data model, and representations, 2022, Accessed: 2022-03-23. [Online]. Available: <https://www.w3.org/TR/did-core/>.

- [107] M. Sporny, G. Noble, D. Longley, D.C. Burnett, B. Zundel, K. Den Hartog, Verifiable credentials data model v1.1, 2022, Accessed: 2022-03-23. [Online]. Available: <https://www.w3.org/TR/vc-data-model/>.
- [108] P.J. Windley, Multisource digital identity, *IEEE Internet Comput.* 23 (5) (2019) 8–17.
- [109] P. Dunphy, F.A.P. Petitcolas, A first look at identity management schemes on the blockchain, *IEEE Secur. Priv.* 16 (4) (2018) 20–29.
- [110] Microsoft, Decentralized identity, own and control your identity, 2018, <https://microsoft.com/ownyouridentity>.
- [111] M. Zervaki, Regulating the IoT: 2020 and beyond, 2020, Accessed: 2020-10-20. [Online]. Available: <https://www.accesspartnership.com/cms/access-content/uploads/2020/06/Regulating-the-IoT-2020-and-beyond.pdf>.
- [112] European Union, General data protection regulation, 2020, Accessed: 2020-10-29. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>.
- [113] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, E.K. Markakis, A survey on the internet of things (IoT) forensics: Challenges, approaches, and open issues, *IEEE Commun. Surv. Tutor.* 22 (2) (2020) 1191–1221.
- [114] E. Oriwoh, D. Jazani, G. Epiphaniou, P. Sant, Internet of things forensics: Challenges and approaches, in: 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing, 2013, pp. 608–615.
- [115] J. Hou, Y. Li, J. Yu, W. Shi, A survey on digital forensics in internet of things, *IEEE Internet Things J.* 7 (1) (2020) 1–15.
- [116] S. Zawoad, R. Hasan, FAIoT: Towards building a forensics aware eco system for the internet of things, in: 2015 IEEE International Conference on Services Computing, 2015, pp. 279–284.
- [117] L. Sadineni, E. Pilli, R.B. Battula, A holistic forensic model for the internet of things, in: IFIP International Conference on Digital Forensics, Springer, 2019, pp. 3–18.
- [118] M. Hossain, Towards a Holistic Framework for Secure, Privacy-Aware, and Trustworthy Internet of Things Using Resource-Efficient Cryptographic Schemes (Ph.D. dissertation), The University of Alabama at Birmingham, 2018.
- [119] H. Chung, J. Park, S. Lee, Digital forensic approaches for Amazon Alexa ecosystem, *Digit. Investig.* 22 (2017) 15–25.
- [120] M. Al-Sharrah, A. Salman, I. Ahmad, Watch your smartwatch, in: 2018 International Conference on Computing Sciences and Engineering (ICCSE), 2018, pp. 1–5.
- [121] S. Symington, W. Polk, M. Souppaya, Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management (Draft), Tech. Rep., National Institute of Standards and Technology, 2020.
- [122] M. Malik, M. Dutta, J. Granjal, A survey of key bootstrapping protocols based on public key cryptography in the internet of things, *IEEE Access* 7 (2019) 27443–27464.
- [123] BITAG, BITAG, 2020, Accessed: 2020-12-16. [Online]. Available: <https://www.bitag.org/report-internet-of-things-security-privacy-recommendations.php>.
- [124] CSA, CSA IoT security controls framework, 2020, Accessed: 2020-12-16. [Online]. Available: <https://cloudsecurityalliance.org/artifacts/iot-security-controls-framework>.
- [125] NIST, NIST IoT security, 2020, Accessed: 2020-12-16. [Online]. Available: <https://www.nist.gov/internet-things-io>.
- [126] Homeland Security, Homeland security IoT, 2020, Accessed: 2020-12-16. [Online]. Available: <https://www.dhs.gov/securingthelot>.
- [127] ENISA, ENISA security IoT, 2020, Accessed: 2020-12-16. [Online]. Available: <https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things>.
- [128] IETF, Who we are, 2020, Accessed: 2020-12-16. [Online]. Available: <https://www.ietf.org/about/who/>.
- [129] E. Lear, R. Droms, D. Romascanu, Manufacturer usage description specification, 2019, Accessed: 2020-12-16. [Online]. Available: <https://tools.ietf.org/pdf/rfc8520>.
- [130] L. Su, MUD is officially approved by IETF as an internet standard, and cisco is launching MUD1.0 to protect your IoT devices, 2019, Accessed: 2020-12-16. [Online]. Available: <https://blogs.cisco.com/security/mud-is-officially-approved-by-ietf-as-an-internet-standard-and-cisco-is-launching-mud1-0-to-protect-your-iot-devices>.
- [131] GSMA, About us, 2020, Accessed: 2020-12-16. [Online]. Available: <https://www.gsma.com/aboutus/>.
- [132] GSMA, GSMA IoT security guidelines, 2020, Accessed: 2020-12-16. [Online]. Available: <https://www.gsma.com/iot/iot-security/iot-security-guidelines/>.
- [133] A. Alhowaide, I. Alsmadi, J. Tang, Ensemble detection model for IoT IDS, *Internet Things* 16 (2021) 100435, [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2542660521000792>.
- [134] ARMIS, INC, Agentless security for the enterprise of things, 2020, Accessed: 2020-11-11. [Online]. Available: https://info.armis.com/rs/645-PDC-047/images/Armis_Solution_Brief.pdf.
- [135] Bastille Networks Internet Security, Bastille, 2020, Accessed: 2020-12-15. [Online]. Available: <https://www.bastille.net/>.
- [136] ReFirm Labs, Centrifuge platform, 2020, Accessed: 2020-11-12. [Online]. Available: <https://www.refirmlabs.com/centrifuge-platform/>.
- [137] Raspberry Pi Foundation, Raspberry pi, 2020, Accessed: 2020-12-16. [Online]. Available: <https://www.raspberrypi.org/products/raspberry-pi-4-model-b/>.
- [138] Zymbit, Zymkey, 2020, Accessed: 2020-12-15. [Online]. Available: <https://www.zymbit.com/zymkey/>.
- [139] Amazon, AWS IoT device defender, 2020, Accessed: 2020-12-16. [Online]. Available: <https://aws.amazon.com/iot-device-defender/>.
- [140] Google, Google IoT core, 2020, Accessed: 2020-12-16. [Online]. Available: <https://cloud.google.com/iot-core/>.
- [141] Microsoft, Azure defender for IoT, 2020, Accessed: 2020-12-16. [Online]. Available: <https://azure.microsoft.com/en-us/services/azure-defender-for-iot/>.
- [142] IBM, IBM IoT platform, 2020, Accessed: 2020-12-16. [Online]. Available: <https://www.ibm.com/business-operations/iot-platform/>.
- [143] Bitdefender, Bitdefender BOX, 2020, Accessed: 2020-11-12. [Online]. Available: <https://www.bitdefender.com/box/>.
- [144] H. Tankovska, Consumer spending on smart home systems worldwide from 2014 to 2023, 2020, Accessed: 2020-12-10. [Online]. Available: <https://www.statista.com/statistics/693303/smart-home-consumer-spending-worldwide/>.
- [145] Statista Research Department, Industrial internet of things market size worldwide from 2017 to 2025*, 2020, Accessed: 2020-12-10. [Online]. Available: <https://www.statista.com/statistics/611004/global-industrial-internet-of-things-market-size/>.
- [146] ipropertymanagement.com, Global IoT market distribution in 2019, by sector, 2020, Accessed: 2020-12-16. [Online]. Available: <https://www.statista.com/statistics/1095380/global-iot-market-distribution-by-sector/>.
- [147] theinsightpartners.com, Size of the internet of things (IoT) security market worldwide from 2016 to 2025, 2017, Accessed: 2020-12-10. [Online]. Available: <https://www.statista.com/statistics/993789/worldwide-internet-of-things-security-market-size/>.
- [148] Markets and Markets, IoT security market, 2020, Accessed: 2020-11-12. [Online]. Available: <https://www.marketsandmarkets.com/Market-Reports/iot-security-market-67064836.html>.
- [149] National Institute of Standards and Technology, Vulnerability metrics, in: National Vulnerability Database, 2020, Accessed: 2020-12-17. [Online]. Available: <https://nvd.nist.gov/vuln-metrics/cvss>.
- [150] MITRE Corporation, Vulnerabilities by type, in: CVE Details, 2019, Accessed: 2020-12-27. [Online]. Available: <https://www.cvedetails.com/vulnerabilities-by-types.php>.