Internet of Things: A Model for Cybersecurity Standards and the Categorisation of Devices

Dissertation

zur Erlangung des Grades eines
Doktors der Naturwissenschaften (Dr. rer. nat.)
am Fachbereich Mathematik und Informatik
der Freien Universität Berlin

von

Sebastian Fischer

Berlin
Dezember 2022

Erstgutachter:	Prof. Dr. Marian Margraf
Zweitgutachter:	Prof. Dr. Rudolf Hackenberg
Tag der Disputation:	13.12.2022

Erklärung

Ich erkläre gegenüber der Freien Universität Berlin, dass ich die vorliegende Dissertation selbstständig und ohne Benutzung anderer als der angegebenen Quellen und Hilfsmittel angefertigt habe. Die vorliegende Arbeit ist frei von Plagiaten. Alle Ausführungen, die wörtlich oder inhaltlich aus anderen Schriften entnommen sind, habe ich als solche kenntlich gemacht. Diese Dissertation wurde in gleicher oder ähnlicher Form noch in keinem früheren Promotionsverfahren eingereicht.

Mit einer Prüfung meiner Arbeit durch ein Plagiatsprüfungsprogramm erkläre ich mich einverstanden.

Berlin, 15. Dezember 2022

Sebastian Fischer

Abstract

The networking of physical devices, including their infrastructure and data, is known as the Internet of Things. The number of networked devices is constantly increasing over the last years and is expected to continue to rise in the future. This also results in an increasing number of attacks on these devices which are considered potentially insecure. The reasons for the lack of cybersecurity are diverse and lead, for example, to botnets and similar problems.

Mandatory standards and guidelines can help to ensure cybersecurity regardless of a fast pace of development and a low price of the devices. In some areas, the development of these guidelines is already well advanced, ideally across countries as a European standard. However, problems with standardization are the different definitions of device categories and thus, the assignment of a device to a standard.

Even in academia, definitions and categories for Internet of Things devices are ambiguous or completely lacking. This makes it difficult to find relevant publications. Therefore, a model of the Internet of Things was researched to solve these problems and define clear categories.

The model divides the Internet of Things into categories, supplements the definitions with characteristics and distinguishes the different device types. The architectures and associated components are also considered. The model can be applied to all devices and available cybersecurity standards which is shown by mapping them to the model. The real-world applications are diverse and illustrated as different use cases. As digitalization evolves rapidly, the researched model is designed to adapt flexibly to new developments.

Acknowledgement

I would like to thank Prof. Dr. Margraf and Prof. Dr. Rudolf Hackenberg for their supervision, support, and feedback during this thesis. Additionally, my parents, my brother and all my friends (including Rocky) for their support the whole time.

Publications

The following related publications were published during this work:

- B. Weber, L. Hinterberger, S. Fischer, R. Hackenberg (2021)
  How to Prevent Misuse of IoTAG?
  CLOUD COMPUTING 2021, The Twelfth International Conference on Cloud Computing, GRIDs, and Virtualization
  ISBN: 978-1-61208-845-7 [1]
  Best Paper Award

- S. Fischer, K. Neubauer, R. Hackenberg (2020)
  A study about the different categories of IoT in scientific publications
  CLOUD COMPUTING 2020, The Eleventh International Conference on Cloud Computing, GRIDs, and Virtualization
  ISBN: 978-1-61208-778-8 [2]

- L. Hinterberger, S. Fischer, B. Weber, K. Neubauer, R. Hackenberg (2020)
  IoT Device IdentificAtion and RecoGnition (IoTAG)
  CLOUD COMPUTING 2020, The Eleventh International Conference on Cloud Computing, GRIDs, and Virtualization
  ISBN: 978-1-61208-778-8 [3]

- L. Hinterberger, S. Fischer, B. Weber, K. Neubauer, R. Hackenberg (2020)
  Extended Definition of the Proposed Open Standard for IoT Device IdentificAtion and RecoGnition (IoTAG)
  International Journal On Advances in Internet Technology, v 13 n 3&4 2020
  ISSN: 1942-2652 [4]

- K. Neubauer, S. Fischer, R. Hackenberg (2020)
  Security Risk Analysis of the Cloud Infrastructure of Smart Grid and IoT - 4-Level-Trust-Model as a Security Solution
  International Journal On Advances in Internet Technology, v 13 n 1&2 2020
  ISSN: 1942-2652 [5]

- J. Graf, K. Neubauer, S. Fischer, R. Hackenberg (2020)
  Architecture of an Intelligent Intrusion Detection System for Smart Home
  IEEE PerCom 2020, 18th International Conference on Pervasive Computing and Communications
  ISBN: 978-1-7281-4716-1 [6]

- S. Fischer, K. Neubauer, L. Hinterberger, B. Weber, R. Hackenberg (2019)
  IoTAG: An Open Standard for IoT Device IdentificAtion and RecoGnition
  SECUREWARE 2019, The Thirteenth International Conference on E-merging Security Information, Systems and Technologies
  ISBN: 978-1-61208-746-7 [7]

- K. Neubauer, S. Fischer, R. Hackenberg (2019)
  Work in Progress: Security Analysis for Safety-critical Systems: Smart Grid and IoT
  ARCS 2019 - 32nd International Conference on Architecture of Computing Systems
  ISBN: 978-3-8007-4957-7 [8]

- K. Neubauer, S. Fischer, R. Hackenberg (2019)
  Risk Analysis of the Cloud Infrastructure of Smart Grid and Internet of Things
  CLOUD COMPUTING 2019, The Tenth International Conference on Cloud Computing, GRIDs, and Virtualization
  ISBN: 978-1-61208-703-0 [9]
  Best Paper Award

Furthermore, contributions (knowledge and participation) to the two standards were brought in:

- DIN SPEC 27072 (as member of the workgroup NIA 41-01 from DIN)
- ETSI EN 303 645 (as member of the CEN-CLC-JTC13)

Finally, some presentations were given at the following events:

- 27.04.2022 **A Security-, Privacy- and Usability- Scoring System for IoT Devices**, CLOUD COMPUTING, The Thirteenth International Conference on Cloud Computing, GRIDs, and Virtualization 2022 [10]
- 03.03.2020 **Security-Mindestanforderungen und -Standards für IoT**, buildingIoT 2020 [11]
- 25.10.2019 **Kategorisierung von IoT Geräten für IT-Sicherheitsstandards**, Gesellschaft für Informatik - Thementag: Sichere Hardware [12]
- 24.01.2018 **IT- Sicherheitsanforderungen im Bereich IoT**, Omnisecure 2018 [13]

Contents

List of Figures

List of Tables

List of Abbreviations

AAL	Ambient Assisted Living
AI	Artificial Intelligence
B2B	Business-to-business
BSI	Federal Office for Information Security
CC	Common Criteria
CD	Constrained Device
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CIoT	Consumer Internet of Things
C-V2X	Cellular Vehicle-to-everything
DD	Default Device
DIN	Deutsches Institut für Normung e. V.
DKE	Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE
EIoT	Enterprise Internet of Things
EN	European Standard
ENISA	European Union Agency for Cybersecurity
ETSI	European Telecommunications Standards Institute
GDPR	General Data Protection Regulation
HTTP(S)	Hypertext Transfer Protocol (Secure)
ICT	Information and communications technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IIoT	Industrial Internet of Things
IoT	Internet of Things
IoTAG	IoT Device IdentificAtion and RecoGnition
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technologie
JSON	JavaScript Object Notation
LAN	Local Area Network
LoRaWAN	Long Range Wide Area Network

MQTT	Message Queuing Telemetry Transport
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency or Internal Report
OWASP	The Open Web Application Security Project
RFC	Request for Comments
TPM	Trusted Platform Module
TR	Technische Richtlinie
URL	Uniform Resource Locator
V2X	Vehicle-to-everything
VDE	Verband der Elektrotechnik Elektronik Informationstechnik e. V.
WAN	Wide Area Network
XD	Complex Device

1 Introduction

Due to many security incidents with Internet of Things (IoT) devices, it was the motivation to explore the topic in more detail in this thesis. Why are IoT devices so insecure in terms of cybersecurity and what solutions can help to make them more secure? These questions have led to the research of a model for the IoT world, which can be used for cybersecurity standards and the classification of devices.

The thesis is structured as follows: First, the existing definitions are explained and example environments are developed, which are used later in the work. Then, cybersecurity in the IoT is further analyzed. Problems are identified as well as solutions are evaluated. One possible solution are cybersecurity standards. A selection of these are presented and evaluated. This results in the Problem Statement. Related Work is then summarized to define the current state of research. In the next step, the model is researched and defined. Followed by the mapping to the real world and the evaluation. At the end of the thesis, further research is presented and a conclusion is drawn.

1.1 Definitions

The important phrases and terms for this thesis are defined below. Only the relevant ones in relation to the researched model are considered.

1.1.1 Internet of Things

The term Internet of Things, short IoT, describes devices, which are connected over the Internet (or a similar network) to an infrastructure of services to monitor or change the behaviour of the device. Because the Internet is difficult to define, the ISO/IEC 20924:2018 (Information technology — Internet of Things (IoT) — Vocabulary) uses the following definition for IoT:

> “infrastructure of interconnected entities, people, systems and information resources together with services which processes and reacts to information from the physical world and virtual world” [14, p. 9]

In difference to the first definition, this one is not limited to devices and the Internet is simplified to interconnected.

This definition leads to a broad variety of included devices. All devices, which can be connected to a network are in scope. This includes connected cars, smart assistants, connected medical devices, airplanes, personal computers, smartphones, smart refrigerators, etc. Additional, to the devices, the whole IoT platform and infrastructure (cloud services, software, etc.) are also in scope.

In this work, the ISO/IEC 20924:2018 definition is used, due to its international validity. If there are meanderings, the corresponding definition will be given.

1.1.2 IoT Device

The IoT device itself is defined in the ISO/IEC 20924:2018 as follows:

> "entity of an IoT system that interacts and communicates with the physical world through sensing or actuating" [14, p. 9]

The device can be a sensor or actuator and has to be connected to a digital entity. No additional (cloud) platforms or software outside of the device are included.

1.1.3 Industrial IoT and Industry 4.0

An already established term is the Industrial IoT, short IIoT. It refers to connected devices in an industrial and production environment, like (smart) manufacturing [15]. Before the term IIoT was used, it was known as Industry 4.0 (the Fourth Industrial Revolution), which describes the further automation by connecting the individual machines [16]. The European Union Agency for Cybersecurity (ENISA) uses the following definition in their report about "Good practices for security of IoT" for Industry 4.0:

> "a paradigm shift towards digitalised, integrated and smart value chains enabling distributed decision-making in production by incorporating new cyber-physical technologies such as IoT" [17, p. 12]

1.1.4 Enterprise

Enterprise is used in the context of commercial, or as "a commercial or industrial undertaking" as defined in the Oxford English Dictionary [18]. It classifies products for the non-consumer market (see chapter 6.3.3).

1.1.5 Consumer

A consumer is defined as an end user, which purchases goods or services [19]. In the context of this work, it is assumed that they do not have extensive Information Technologie (IT) knowledge. This means that manufacturers of devices, designed for consumers, cannot expect them to have extensive expertise in the area of IT and, in particular, cybersecurity.

1.1.6 Smart Home

Smart home or home automation refers to the networking of devices in the home with each other, or with the Internet [20]. Smart home is thus a part of IoT. Typical devices include smart refrigerators, voice assistants, smart TVs, etc. The common used designation “smart” indicates that these devices are networked.

1.1.7 Smart City

Smart city summarises technological developments that provide for the improvement of cities [21]. These include networked street lights, intelligent parking systems, digital administration, etc. Since the driving force is also networking, the technologies also belong to the IoT.

1.1.8 Edge Computing

In edge computing, all or part of the data processing is performed at the data source [22]. There are several ways to do this. For example, an IoT device can process the data before it is sent to a data center in the cloud. This helps to save resources in the data center, as well as bandwidth, since not all data, but only results are sent.

Another possibility is the calculation in the local network via own edge servers before the results end up in the cloud. In this case, the data remains in the companies own network and the results can still be made accessible via the Internet.

In principle, the goal of edge computing is always to perform the calculation closer to the source, either to shift the computing load, or to save transmission bandwidth.

1.1.9 Third-party Software

Third-party software is defined as “computer programs that are supplied or developed for a particular purpose by a different company from the one that supplied or developed the existing programs on a particular system” [23]. In this thesis, a software is considered as a third-party software, if the software is not preinstalled by the manufacturer of the IoT device at the time of purchase.

1.2 The Growing Role of IoT

Due to the broad definition of IoT (see chapter 1.1.1), the digitalization of all areas counts as part of the Internet of Things. A survery from Statista [24] counts 7.7 billion connected devices worldwide in the year 2019. The number is increasing to estimated 25.4 billion in 2030. The consumer sector is forecast to triple from 2019 to 2030. The worldwide spending on the IoT increased from 646 billion U.S. dollars in 2018 to 749 billion U.S. dollars in 2020 and is forecasted to 1,100 billion U.S. dollars in 2023 [25]. By 2030, the global value of IoT is estimated by 5.5 trillion to 12.6 trillion U.S. dollars (consumer, enterprise and industrial) in a research report by McKinsey [26]. Business-to-business applications account for about 65 percent of the potential of the IoT, followed by Human Health and Consumer [27, p. 10].

The increasing numbers in the consumer sector state out the important role and huge impact on private life. This creates a dependency on the used technologies. In the event of malfunctions or attacks from outside, the potential damage increases with the higher number of devices. Depending on the type of device, this can also have health implications as shown in chapter 2.3.

The number of networked devices is also increasing in the enterprise sector. Analogous to the consumer sector, the damage is also increasing with the number of devices. This can have a greater impact, as the damage potential is much higher than in private households. This applies equally to the industrial sector in the event of production stoppages or safety incidents, as well as, in the case of critical infrastructures.

Since this thesis is about cybersecurity, the current situation will be briefly presented using data from the 2021 Situation Report by the Federal Office for Information Security (BSI) [28]. In summary, the BSI rates the IT security situation as tense to critical. On the one hand, this is due to the fact that an average of 394,000 new variants of malware became known every day. On the other hand, it is due to the advanced nature of the malware. Protection money (e.g., DoS protection), ransomware and blackmail are the result. The IoT plays a major role in this, as more and more connected devices enter the market and the attack surface increases. It also increases the number of potentially insecure devices, as evidenced by the peak bot infection of 40,000 devices per day.

Further on the topic of IoT device security, a survey by the Internet Society shows that 88 percent of the asked consumer agree with the following statement: “There should be legal privacy and security standards that manufacturers need to comply with”, in turn, only 60 percent agree with the statement “Consumers are mainly responsible for their own privacy and security when using connected devices” [29, p. 12]. This means, some consumers see it as the manufacturers’ responsibility to pay attention to privacy and security. Which makes sense, since a normal user does not have extensive IT knowledge.

1.3 Example Environments

This chapter shows some examples of IoT devices and the environment they are connected to. The background of this chapter is to show which different types of IoT devices exist. Especially, the different environments are important, since IoT is present in private, corporate and public environments. The examples are used at the end of the thesis to validate the researched model.

In selecting the devices, care was taken to ensure that some devices allowed for many possibilities and were often difficult to place in a single category. For example, a networked baking oven can be placed in a private or business environment.

1.3.1 Smart Home

A smart home network connects individual intelligent devices in the private household. The example environment for a typical smart home includes several consumer products, like:

- Smart Assistant
- Smart TV
- Smart Fridge
- Robot Vacuum Cleaner
- Smartphone
- Desktop Computer
- Router
- Smart Control Hub

It can be extended with some Smart Building devices, which can be found in a smart home or an office environment:

- Smart Lighting
- Smart Lock
- Window Sensor
- Smart Meter

These devices are difficult to categorize, as, for example, smart lighting can be used in an apartment or office space. The devices described are shown in Figure 1.1 which also includes the exemplary connections.

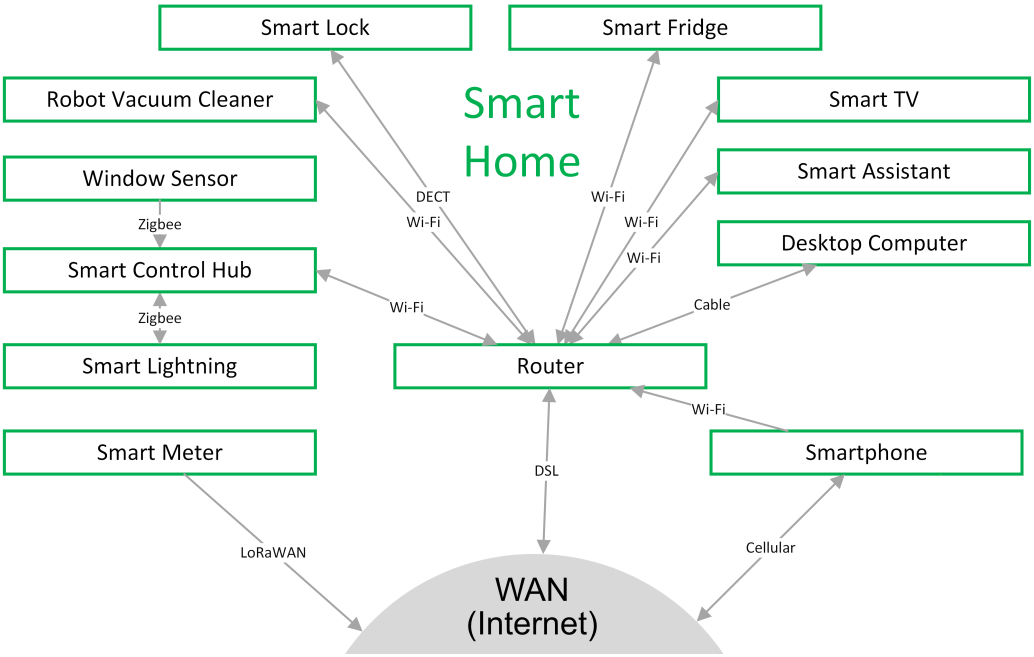


Figure 1.1: Smart Home Example Network

There are different kinds of connection technologies for the smart home devices (mostly wireless): Zigbee, DECT, Wi-Fi, Cellular, LoRaWAN, DSL and (Ethernet) Cable. This list can be extended with more technologies, as the smart home market is big.

1.3.2 Wearables

Wearables are devices that are intended to be worn on the body. Special attention is paid to the data that can be collected with them. These can provide information about a person's physical health. In some cases, experiments are even being conducted to determine whether a person's mental state can also be diagnosed with a smartwatch [30].

There are two devices in the example architecture:

- Smart Watch
- Fitness Tracker

Connectivity is straightforward and can be seen in Figure 1.2.

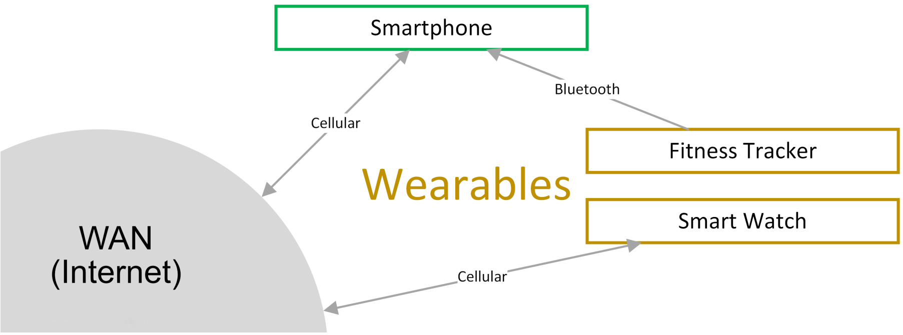


Figure 1.2: Wearables Example Network

Usually, they communicate over Bluetooth, Wi-Fi or directly to the Internet via cellular network.

1.3.3 Automotive

A vehicle can also be seen as an IoT device, since a modern car has several ways to communicate with the outside world. In most cases, the connection is established via the cellular network (2G, 3G, etc.). This means that the Internet can be used to offer different services, e.g., to retrieve navigation and traffic data.

Another connection option incorporates the pairing with the user's smartphone. In this case, applications, data and the Internet connection from the cell phone are used in the vehicle.

As third possibility, Vehicle-to-everything (V2X) communication can be used [31]. In this case, several vehicles communicate with each other (Vehicle-to-Vehicle) via a defined standard, e.g., to provide information about dangers or road conditions. If the communication is extended to other devices, it is referred to as V2X communication. Further devices can be, for example, a traffic light system, which informs the car how long a current traffic light phase will last. It is possible to extend the range of V2X communication using each participant as an amplifier to pass on the information to the respective communication partners that can be reached (mesh network).

The automotive sector includes the following sample devices:

- Car
- GPS Tracker
- Traffic Lights
- Parking Space Sensor

The automotive and V2X architecture is shown in Figure 1.3. The two parts, “Parking Space Sensor” and “Traffic Lights” are also part of smart city (as indicated by the two colors).

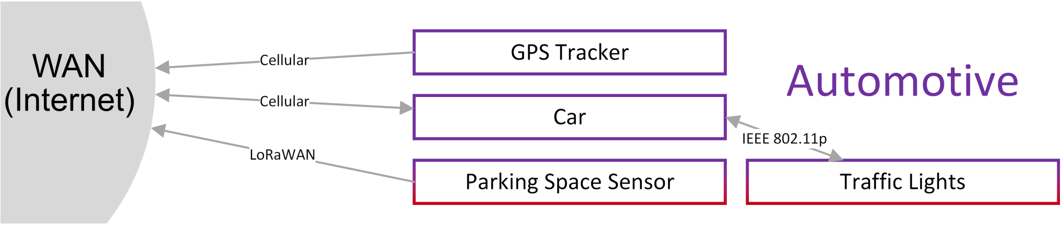


Figure 1.3: Automotive Example Network

In this example, the technology IEEE 802.11p (pWLAN in German) is used to connect the different devices. There are currently two competing standards, Cellular V2X (C-V2X) and the already mentioned IEEE 802.11p. C-V2X is based on the cellular network and developed by the 3rd Generation Partnership Project [32]. As the IEEE 802.11 standard describes the wireless network protocol Wi-Fi, the extension 802.11p is based on this protocol family [33].

The Federal Communications Commission, as a regulation agency of the United States government, has in the meantime released the radio spectrum of IEEE 802.11p for other uses and thus opted for C-V2X. However, some car manufacturers still rely on the 802.11p standard and applications are already being tested in Germany [34]. For example, the construction site warnings of Autobahn GmbH, which were announced on April 29, 2021 [35] [36].

1.3.4 Smart City

Since smart city describes not only devices, but the complete digitalization of cities, many terms are counted as smart city:

- Public administration
- Housing
- Health
- Local transport
- Energy
- Buildings
- Logistics
- Farming
- Security
- Hospitality
- Education

These terms are only generic. For the smart city example, the following concrete devices are used:

- Garbage Can Sensor
- Smart Street Lights
- Visitor Counter
- Parking Space Sensor
- Traffic Lights

There are only five example devices, because individual areas of smart home, health, industrial, enterprise, etc. are also part of smart cities and already covered in the other examples.

The architecture and connections can be seen in Figure 1.4. Two of the devices (Parking Space Sensor and Traffic Lights) are also part of automotive (as indicated by the two colors). For this reason, the car is also in the figure to complete the communication-path.

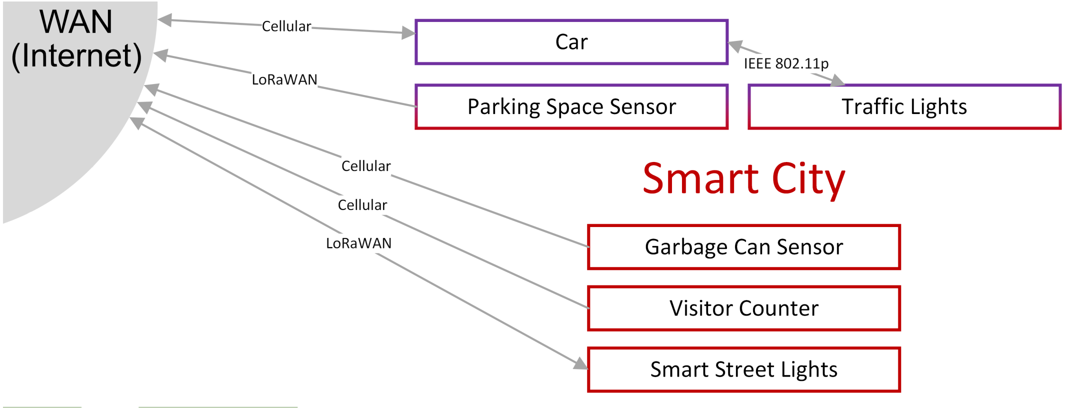


Figure 1.4: Smart City Example Network

LoRaWAN, Cellular and IEEE 802.11p are examples used for communication.

1.3.5 Health

The collective term health covers devices that are used in the medical sector and have been enhanced with an additional interface for a communication capability. The devices can be used in doctors' offices, in hospitals, as well as at the patients' home.

Since there is the possibility to gain very private data, and health can be affected by a failure or a change in the functioning of the devices, the focus should be placed on security and safety.

The following devices are representatives for the health sector:

- Heart Pacemaker
- Fall Sensor
- Insulin Pump
- Blood Glucose Meter
- Medical Monitoring Device

The connections can be seen in Figure 1.5. Depending on the area of application, the connection is directly to the Internet or via a gateway

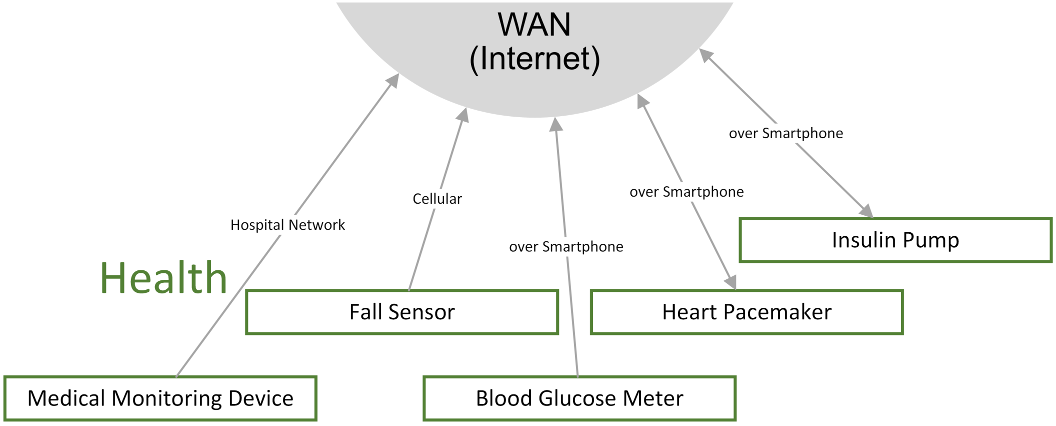


Figure 1.5: Health Example Network

In the case of hospital devices, the connection to the Internet is established over the hospital network, in other cases it can be directly (via Cellular) or, over a Smartphone.

1.3.6 Enterprise

The enterprise sector includes a lot of uses cases for IoT, as nearly every network with connected devices can be called IoT. One way of defining the term is, to include only devices that are not usually networked, but will be integrated into a network in the future, to create new added values. A bakery is used as an example. The oven can be networked to enable control via app and thus create added value because monitoring can happen automatically.

The other selected devices are often difficult to assign explicitly to the enterprise area, since they can also be found in a smart home environment. This has the advantage that these borderline cases are also considered later when assigning them to the researched model. The following devices are examples:

- Networked Baking Oven
- Temperature Sensor
- Smart Lighting
- Online Cash Register System
- Workstation

The connection is typically over the company network. In some cases, a direct connection (e.g., over Cellular or LoRaWAN) is possible. The example connections can be seen in Figure 1.6.

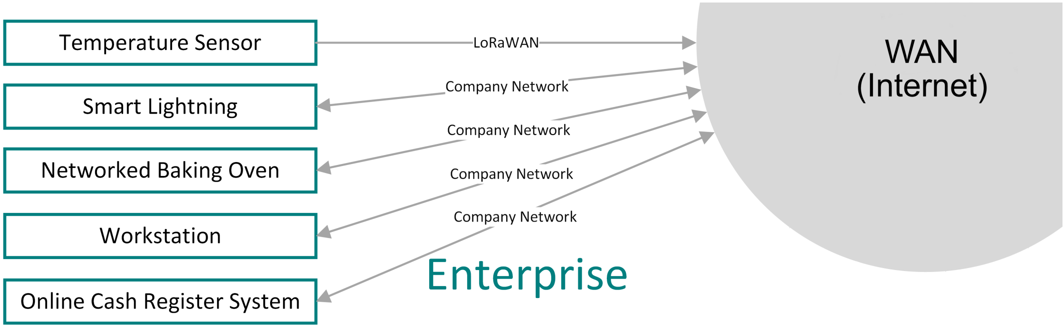


Figure 1.6: Enterprise Example Network

1.3.7 Industrial

Industrial IoT usually involves many sensors, controllers and networked machines. They are all in the production hall and not the office. Depending on the level of automation, there can be several hundreds or even thousands. The challenge with IIoT is rather the number of devices and not the diversity. A possible architecture and the connections can be seen in Figure 1.7.

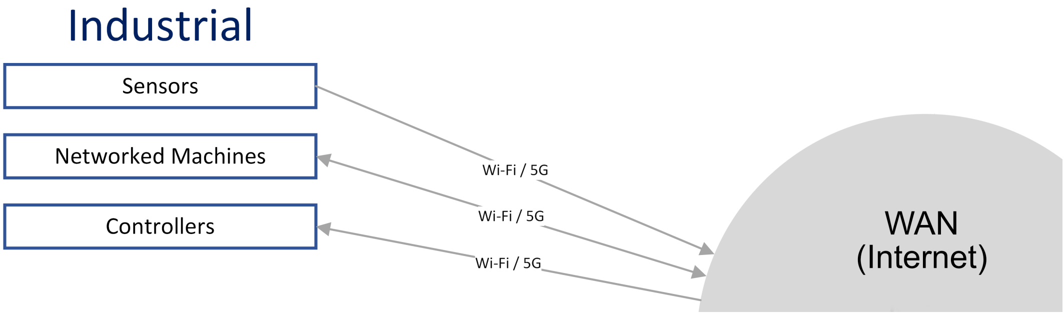


Figure 1.7: Industrial Example Network

Typically, the communication is straightforward with Wi-Fi or 5G to the factory network and then, if necessary, preprocessed and finally sent to the Internet.

1.4 Summary

The examples show that the IoT encompasses a wide range of devices and areas. The classification into smart home, wearables, automotive, smart city, health, enterprise and industrial is common and widespread. A precise definition is not necessary, as the examples only serve to validate the researched model in chapter 7.2.

The complete overview of all areas can be found in Figure 1.8. The Internet serves as the central point. Equivalent to the individual areas, communication is also shown. A larger version of the figure can be found in the appendix 11.1.

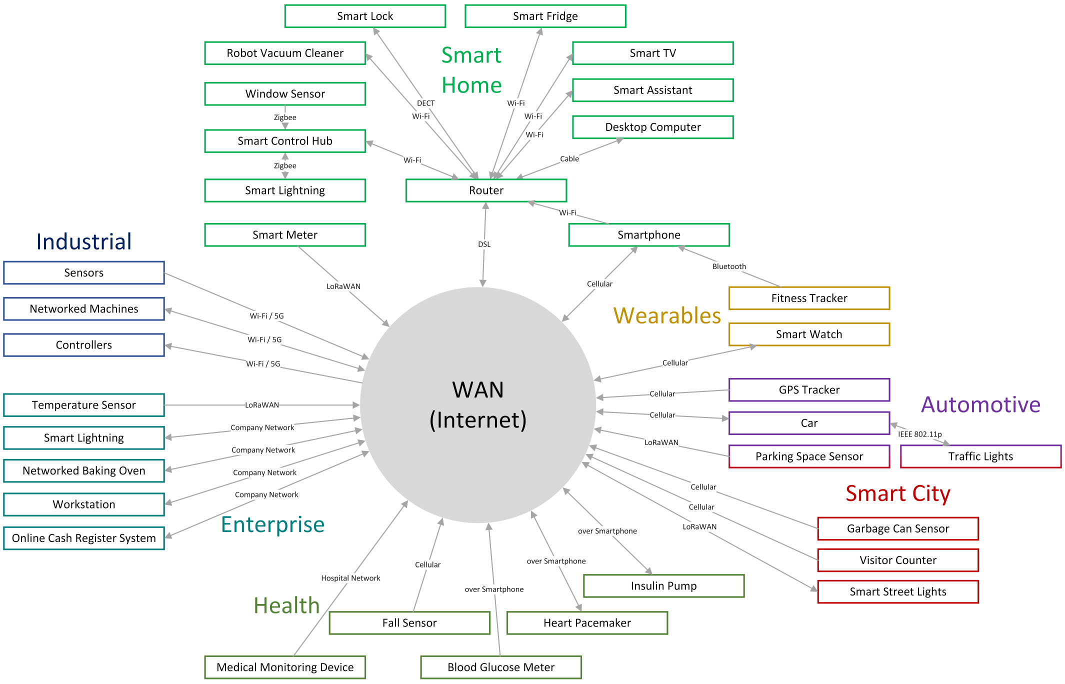


Figure 1.8: Big Picture - IoT Network

2 Cybersecurity in the IoT

In this chapter, the missing cybersecurity in the field of the IoT is shown. Due to the widespread use of IoT (see chapter 1.2), there are increasing problems with security, which are described in the first parts. In the following part, the dangers of the missing cybersecurity are identified. Possible solutions are presented in the last part and a concrete method for finding insecure devices is discussed in more detail at the end.

2.1 Security Issues

This chapter shows the security problems of IoT devices by means of a report on Germany and an overview of several security incidents within four years.

The "Bericht zum Digitalen Verbraucherschutz 2020" (Digital Consumer Protection Report) [37] shows the development of digitalization in Germany via several consumer surveys and studies on the topic. In the process, a number of security incidents in the IoT area were also identified in 2020. This concerns not only security-relevant devices, such as networked doorbells, but also children's toys [37, p. 16]. It is becoming clear that children's data is also being collected and analyzed and is thus also becoming the target of attackers. It is further mentioned that especially in the field of IoT, the principle of security by design is neglected [37, p. 18]. One presented possible solution is the use of standards, which are intended to encourage manufacturers to improve IT security. Reference is made to the ETSI EN 303 645 standard [37, p. 25].

In the years from 2017 to 2020, a lot of security problems occurred with IoT devices. Some selected issues are collected in Table 2.1.

Table 2.1 starts with FOSCAM, a vulnerability for Internet Protocol (short IP, described in RFC 760 [53]) security cameras. When used with the default configuration, it was possible to access the internal memory and the configuration page without any password [38]. The second, third and fourth entries in Table 2.1 (Hide'n Seek, OMG and TORII) are botnets, which spread over a lot of IoT devices by using default credentials, dictionary attacks or Brute-Force to extend their network of hacked devices [39, 40, 41]. The Smart Grid Blackout (fifth entry in Table 2.1) is an article that describes how these botnets can be used to cause a blackout [42].

Table 2.1: Selected Vulnerabilities from 2017 - 2020

Name	Vulnerable Devices	Vulnerability	Date
FOSCAM [38]	IP cameras	Default settings (no password)	8.6.2017
Hide'n Seek: IoT-Botnetz [39]	All kind of IoT devices	Default credentials, Dictionary attacks	25.1.2018
OMG-Botnet [40]	All kind of IoT devices	Brute-Force, Default credentials	28.2.2018
TORII [41]	All kind of IoT devices	Telnet, Default credentials	28.7.2018
Smart Grid Blackout [42]	Smart Grid devices	Different ones (Botnet)	5.4.2019
LinkP2P [43]	All kind of IoT devices	Bad encryption, connection without authentication	29.4.2019
Brickerbot 2.0 [44]	All kind of IoT devices	Default credentials	26.6.2019
Silex [45]	All kind of IoT devices	Default credentials	26.6.2019
Targeted spy attacks [46]	All kind of IoT devices (mainly printer and VoIP-Phones)	Default credentials, missing updates	8.8.2019
Telestar Internetradios [47]	Telestar Internet radio	Open Telnet, Root vulnerable to bruteforce, app sends unencrypted commands via HTTP	11.9.2019
Dahua [48]	IP cameras	Buffer Overflow, open Debugging interface, DoS	15.9.2019
Passwords disclosed [49]	All kind of IoT devices (Mainly Server and Router)	Open Telnet	20.1.2020
Lilin [50]	Video surveillance systems	Command Injection, hard-coded credentials	23.3.2020
Universal-Plug-and-Play-Standard (UPnP) [51]	All kind of IoT devices	UPnP vulnerability	9.6.2020
P2P [52]	All kind of IoT devices	Peer-to-Peer-Protocol vulnerability	9.8.2020

At least three new botnets with IoT devices have been discovered in 2018 alone. Protection against these attacks would be simple, as they always involve default credentials or weak passwords. Insecure software can also be the trigger (see LinkP2P in Table 2.1) [43]. Once the vulnerabilities are known, they are added to the malware repertoire and only an update can help.

The other security problems in Table 2.1 also involve trivial attacks, suggesting that the real problem is a lack of fundamental cybersecurity. For example, Buffer Overflow, open debugging interfaces [48], old protocols like Telnet [47, 49], etc.

Particularly severe cases affect almost all IoT devices, as the last entry shows [52]. Researchers from Forescout Research Lab found 33 vulnerabilities in the TCP/IP stack. They have analysed seven open source stacks which are commonly used by IoT manufacturers [54].

These selected security issues not only concern consumer products. Enterprise and industrial devices are also affected. An Internet scan by researchers at Otori found nearly 70,000 vulnerable industrial control systems in 2021 [55].

2.2 OWASP Top 10 IoT

As shown in the previous chapter 2.1, there are a lot of vulnerabilities in IoT devices. The Open Web Application Security Project (OWASP) describes the top 10 IoT vulnerabilities in their Internet of Things Project [56], to give a brief overview of the cybersecurity problems:

1. **Weak, Guessable, or Hardcoded Passwords**
   Use of easily bruteforced, publicly available, or unchangeable credentials, including backdoors in firmware or client software that grants unauthorized access to deployed systems.

2. **Insecure Network Services**
   Unneeded or insecure network services running on the device itself, especially those exposed to the Internet, that compromise the confidentiality, integrity/authenticity, or availability of information or allow unauthorized remote control...

3. **Insecure Ecosystem Interfaces**
   Insecure web, backend API, cloud, or mobile interfaces in the ecosystem outside of the device that allows compromise of the device or its related components. Common issues include a lack of authentication/ authorization, lacking or weak encryption, and a lack of input and output filtering.

4. **Lack of Secure Update Mechanism**
   Lack of ability to securely update the device. This includes lack of firmware validation on device, lack of secure delivery (un-encrypted in transit), lack of anti-rollback mechanisms, and lack of notifications of security changes due to updates.

5. **Use of Insecure or Outdated Components**
   Use of deprecated or insecure software components/libraries that could allow the device to be compromised. This includes insecure customization of operating system platforms, and the use of third-party software or hardware components from a compromised supply chain.

6. **Insufficient Privacy Protection**
   User's personal information stored on the device or in the ecosystem that is used insecurely, improperly, or without permission.

7. **Insecure Data Transfer and Storage**
   Lack of encryption or access control of sensitive data anywhere within the ecosystem, including at rest, in transit, or during processing.

8. **Lack of Device Management**
   Lack of security support on devices deployed in production, including asset management, update management, secure decommissioning, systems monitoring, and response capabilities.

9. **Insecure Default Settings**
   Devices or systems shipped with insecure default settings or lack the ability to make the system more secure by restricting operators from modifying configurations.

10. **Lack of Physical Hardening**
    Lack of physical hardening measures, allowing potential attackers to gain sensitive information that can help in a future remote attack or take local control of the device.

(OWASP Top 10 IoT Vulnerabilities [57])

This overview shows that trivial problems with passwords, services, updates, insecure components and default settings are common [11]. These problems can easily be prevented by following basic principles when developing IoT devices. Choosing a strong password is one of the easiest things to do, and not using hardcoded passwords goes without saying. Insecure, outdated components can also be avoided without much effort during development.

2.3 Threats

With the IoT, new threats emerge. Looking at the characteristics of IoT devices, one can identify these threats. The following properties have an impact on security and therefore pose a new threat. Table 2.2 presents the special characteristics of the IoT, the corresponding devices and threats. A more detailed overview (not restricted to the special characteristics of the IoT) can be found, for example, in the study “Baseline Security Recommendations for IoT” by ENISA, which lists and evaluates the threats in the context of critical information infrastructures [58, pp. 34–35].

Table 2.2: Threats of IoT

Characteristics of IoT	**Example devices**	**Threat**
Big Data	Wearables, smartphones, child toys	Private or personal data can be stolen or published
Safety	Connected cars, connected production machines	Harm to persons or risk of death
Real-time	Traffic light control	The reduction of safety
Scalability	Smart Home	Attack from multiple devices, Denial-of-service attack
Volatility	Sensors, smartphones, connected cars	Traceability, no integrity
Low Price	Sensors, Smart Home	Cheap, insecure devices
External Data	Cloud	No data protection
Low Performance	Sensors	No encryption possible

Big Data: Many devices that normally operate without any electronics are equipped with sensors and a network interface. For example, a wristwatch or a child's toy [59]. These devices collect a lot of data about the use of the device, but also about the user. Thus, with the IoT comes new data, which can include both, private and personal data. This data can be stolen or made public if the device or services are not secured.

Safety: A networked car nowadays consists of over 100 microcontrollers [60]. Not only does this generate a lot of data, but the safety of the driver and other road users also depends on microcontrollers. The IoT thus also influences safety and can cause harm to people. Networked production machines in factories are another example for devices which can cause safety issues for people.

Real-time: Real-time requirements for IoT devices can also influence safety. An intelligent traffic light control system, which has to react quickly enough to provide (autonomous) cars with information about the traffic situation, can be disrupted or influenced by attackers [61].

Scalability: A typical feature of the IoT is its high scalability. There are more and more networked devices. For example, a U.S. household has an average of 25 networked devices [62]. This high number of devices can be used by attackers to build botnets [39, 40, 41]. This allows attacks to be carried out on an increasingly large scale (e.g., denial-of-service attacks).

Volatility: The volatility of IoT devices makes it difficult to ensure the integrity of data. A device may not be identifiable [63]. In this case, it is no longer possible to determine exactly which device is responsible for which data. An example is a public wireless network. In the case of illegal activity, it becomes difficult to tell which device is responsible, because many devices only connect to it for a short time. However, these short-term connections can also be used for tracking. A smartphone could be tracked by evaluating the connections from different networks and creating a movement profile [64].

Low Price: Due to the low prices of microcontrollers, more and more devices are equipped with microcontrollers. In the process, no money is budgeted for security, because a cheaper device sells better. As a result, insecure devices are coming onto the market [65]. The low price also tempts people to buy a connected product, even if it offers only few advantages.

External Data: The data of the networked devices can be evaluated and it is handy for the user, if he can access it from anywhere via the Internet. Therefore, a cloud is used which takes the data and processes it further. The user must trust the cloud provider that his data is stored securely and provided with sufficient access protection [66]. If an attacker finds a vulnerability in the cloud, all users could be affected and the impact is higher than with local data storage.

Low Performance: The last characteristic of IoT devices concerns the low performance. If a sensor cannot perform complex calculations, it is usually not possible to ensure encryption and secure data communication [67].

If we take the characteristics of IoT together and evaluate the threats, we find that scalability and low price, for example, multiply the threats. A low price means that more devices are networked and sold, but also that less priority is placed on cybersecurity. This leads to a high number of insecure devices and can cause botnets with several million devices as seen in chapter 2.1.

Table 2.3: Risks of the smart grid connected to a IoT network [8, p. 4]

Threat	Ability of an attacker	Damage on smart grid	Risk
IoT Device / IoT Cloud			
Malware on IoT device	medium	high	high
Controlling IoT device	medium	medium	medium
DDoS IoT device	low	medium	medium
Destroy IoT device	medium	low	low
Using IoT device in a botnet	medium	medium	medium
IoT infrastructure			
Control of the the IoT cloud	medium	high	high
Smart Grid			
Attack on smart meter	high	medium	medium
Attack on smart meter gateway	high	high	medium
Attack on switching box	high	medium	medium
Attack on user app	high	high	medium
Attack on value-added services	high	medium	medium
Attack on energy supplier	high	high	medium
Attack on IoT device	medium	medium	medium
Attack on meter data management system	high	high	low
Attack on head end system	high	high	low

IoT poses an increased risk when considering the digitalization of the energy grid (smart grid). The smart grid is a critical infrastructure and its architecture is designed in a way that connections to the gateway administrator are carried out via a dedicated communication channel. However, there is an interface to the smart home via the smart meter gateway to exchange energy data (e.g., the current electricity price). This interface connects the network of the smart grid, which is to be regarded as secure, with the insecure network of the smart home. The individual risks for both infrastructures must be considered as a whole. Table 2.3 shows the risks of different attacks on the IoT environment and the Smart Grid. The risk is based on the ability of an attacker and the possible damage on the smart grid, as the smart grid is in the focus. Possible solutions to this problems are presented in the paper “Work in

Progress: Security Analysis for Safety-critical Systems: Smart Grid and IoT" [8]. The interface must be strictly regulated and secured, an intrusion forecast, detection and prevention system should be used, and a role-based trust model for safety-critical systems is presented, which classifies data according to safety requirements.

The detailed risk analysis and the 4-Level-Trust-Model can be found in the publications [9] and [5]. One method to build an intrusion detection system for smart home using Artificial Intelligence (AI) is described in the paper "Architecture of an intelligent Intrusion Detection System for Smart Home" [6].

2.4 Solutions

Most security problems do not require extensive research for new encryption algorithms or similar. The problems can be solved with conventional cybersecurity, as been practiced for years. There are devices that are limited by their nature and cannot reliably implement all security mechanisms [68], but this only applies to parts of an entire network.

One example is AES symmetric encryption which was classified as secure by the BSI in Technical Guideline 02102-1 "Kryptographische Verfahren: Empfehlungen und Schlüssellängen" [69] with a minimum length of 128 bits. If an IoT device can communicate with the Internet via IP communication, TLS is usually used in a current version (TLS 1.2 or higher). In order to be able to support TLS from version 1.2, AES with a length of 128 bits must also be supported [70]. This means that the hardware is at least designed for such calculations and a missing encryption is not a hardware limitation. If a sensor does not support TLS or does not use IP communication, the data is sent to a gateway which forwards it to the Internet and can thus implement secure messaging (e.g., through an encrypted TLS connection). The connection to the gateway may be not secure, but an attack on multiple devices over the Internet is not possible, only a single attack within radio range.

Another example concerns the pairing process with new devices. If there are limitations with the IoT device due to a lack of input and/or output options, it is often not possible to establish a secure initial connection [71]. There is no user friendly solution for such a secure processes. But due to the fact that this attack cannot be executed en masse over the Internet, as it requires physical access to the device, there is no high risk involved and already proven mechanisms (e.g., the pairing method "Just Work" or "Numeric Comparison" [71]) are sufficient.

The reason for the lack of security in the devices is often the fast development time and the lack of expertise. The products have to be launched on the market as quickly (time to market) and as cheaply as possible, while cybersecurity is neglected [72]. A long-term supply of patches and security updates is expensive and not pursued without necessity [73, p. 17]. There is a lack of incentives for better cybersecurity or penalties for a lack of cybersecurity. Secure products cannot be sold more expensively and there are often no requirements by the legislator.

Because of these reasons, standards are necessary to force manufacturers to comply with at least a minimum level of cybersecurity in their products. Additionally, the standards and guidelines must encourage manufacturers to think about the security of their products and the corresponding data.

The first steps in this direction are currently planned with national and international standards or, in the case of DIN SPEC 27072 and ETSI EN 303 645 (see chapter 3), have already been implemented. Additionally to the baseline security, there is a need for higher level cybersecurity standards to protect critical devices and personal data.

2.5 Identification of Insecure Devices

As seen in the previous chapters, there are enough networks with insecure IoT devices. To secure a network, the first step is to find all insecure devices that they can either be updated or excluded from the network. However, this is not easy in both, private and corporate environments. In private environments, users lack the expertise to identify them, and in companies, there are often too many devices to keep track of. Forgotten or unknowingly connected devices can also cause a security risk.

One approach to solve this problem is a network scan. This scan can be performed with the nmap tool [74], for example. The devices found can then be checked and their security assessed. However, the necessary expertise is required for the whole procedure and it takes time to check all devices individually for updates and possible vulnerabilities in order to make a valid statement about their security.

An automated solution for this procedure (network scan, analysis and evaluation) is being developed with IoTAG at OTH Regensburg and presented in the following chapter.

2.5.1 IoTAG

The IoT Device IdentificAtion and RecoGnition, short IoTAG, describes a solution, where IoT devices provide information about themselves to a central control unit in the network [7]. These information are used to detect all IoT devices in the network and analyse the status of the devices. The IoTAG, send by the devices, contains the following information [3]:

- Manufacturer
- Name
- Serial Number
- Type
- ID
- Category
- SecureBoot
- Firmware
- Client Software (Version, URL, Automatic Updates)
- Cryptography (Software, Hardware)
- Connectivity (IEEE 802.3, Bluetooth, Zigbee, etc.)
- Services

The IoTAG data is generated on the IoT device with the current information and send as a JSON object to the requesting device. These information can be used to check the security state of the device. For example, if there are any outdated encryption algorithms in use or the current firmware version is installed. To check the firmware version, a URL is given which leads to the newest version, provided by the manufacturer. In addition to the current status, security relevant parts of the configuration can also be read out, e.g., whether automatic updates are activated.

Services are another example. If unencrypted or outdated protocols such as the Session Initiation Protocol, Hypertext Transfer Protocol (HTTP) or unencrypted Message Queuing Telemetry Transport (MQTT) are used, it can be considered as a security risk [4]. These can be easily identified and avoided.

One goal of IoTAG is an automated security analysis of all IoT devices in the network. The IoTAG information is to be used to automatically determine if there are security problems or if a device can no longer be operated securely. A simple overview of the network is to be presented in a way that can be understood by a layperson. It is planned to include external sources on vulnerabilities and fill in the missing information via the Internet and the help of the user. In the end, the solution is to be used in private, as well as in enterprise environments. The first focus is on the smart home, where no experts manage the network and most security problems are not fixed (see chapter 2.1).

IoTAG does not only offer advantages. If an attacker gains access to the network, he can retrieve the IoTAG information and also obtain information about the security of the individual devices. To prevent this from being exploited, a pairing process has been developed which ensures that only a trusted device can retrieve the IoTAG. The pairing process is described in a paper from 2021 [1].

The IoTAG solves several problems: it provides an overview and recognition of the devices in the network, gives security-relevant information and can be evaluated automatically. Research is still in its early stages and further research projects will continue to develop it with the goal of it being implemented as a standard by manufacturers. Currently, there are no implementations in products which is why the advantages cannot yet be used.

2.5.2 Existing alternatives to IoTAG

The “IoT Sentinel” project by TU Darmstadt describes a way to identify and categorize IoT devices in a network using a fingerprint, and to classify them as secure or insecure using a central database. The fingerprint is generated by observing the initial network traffic which is identified using 23 parameters. The security is based on the application layer used and the content of the transmitted packets [75].

There are some commercial solutions from cybersecurity companies. NortonLifeLock Inc. offered the Norton Core Router until end of 2019 [76]. This was a hardware-based approach which replaces the router in the home network. This leads to a relatively large range of functions. For example, in addition to device detection and evaluation, the Core Router also offers general monitoring of network traffic using deep packet inspection and intrusion prevention which promises to detect and prevent external attacks on the network. Since this is a proprietary, closed system, it is difficult to describe device detection and rating in more detail due to a lack of information.

The Avira Operations GmbH offers a solution with Avira Safethings. It is designed to extend the router with additionally functionalities [77]. Similar to the Norton Core Router, Avira keeps a low profile regarding the exact function of the rating system, but describes the detection of the devices in much more detail. It relies on three components for this: the examination of the texts/data transmitted by the device, the categorization of devices with the help of a database and the AI-based analysis of the network traffic for known patterns [78].

L. Nagy and A. Coleşa describe a similar approach using a Raspberry Pi as an alternative router with additional software to secure the smart home (IoT) network. They present solutions, e.g., for SQL-injection, DoS and brute-force attacks [79].

2.6 Summary

There are a lot of security issues with IoT devices. As seen with the Vulnerabilities and the OWASP Top 10, trivial problems lead to a high amount of botnets and hacked devices. The impact of these insecure devices ranges from data loss to endangering human lives. Due to the high number of devices and other features of the IoT, the threats are multiplying.

The solution to the security problem is simple: secure development (security by design) and patch-management with ongoing updates. But the manufacturers, who cannot or do not want to implement these solutions, are problematic. Therefore, standards and guidelines must be developed as a help and regulation.

A further solution for detecting insecure devices in a network during operation is already being researched, for example with IoTAG. This provides an opportunity to patch insecure devices or replace them with secure alternatives. In addition to IoTAG, products already exist that offer similar functionality, but these are neither transparent nor can they access additional information from the device.

In summary, it can be said that, in addition to the new functions, the IoT brings many dangers and hazards. These dangers can be reduced by placing more attention on cybersecurity, but this must be made mandatory through standards and guidelines, as currently even trivial vulnerabilities are not avoided without an incentive. In order to operate a network securely with new and existing devices, solutions are currently being developed to assess the security status of a network.

3 Cybersecurity Standards

Currently, there are a lot of regulations, guidelines and standards for cybersecurity for IoT devices. But not all of them have to be applied to every IoT device and infrastructure. This chapter provides a brief overview of some of them, with the definition of IoT devices they are applied on. The selection shows how differently IoT devices are distinguished in terms of performance and affiliation.

Table 3.1 provides an overview of the selected cybersecurity standards, which are mainly for the consumer market. DIN SPEC 27072 and ETSI EN 303 645 are described in more detail in the following chapters, because they contain concrete provisions and the content of which was contributed to within the scope of this work. Some important ones are also mentioned with a short evaluation to show that the topic is currently present in all countries.

Table 3.1: Cybersecurity Standards

Name	**Publisher**	**Validity**
SPEC 27072	DIN	Germany
EN 303 645	ETSI	EU
The Radio Equipment Directive	European Commission	EU
The Common Criteria for Information Technology Security Evaluation	ISO / IEC	Worldwide
The EU Cybersecurity Act	European Commission	EU
General Data Protection Regulation	European Commission	EU
NISTIR 8259	NIST	USA
Regulatory proposal of the UK Government	UK Government	UK
Finnish Cybersecurity label	Traficom	Finland

3.1 DIN SPEC 27072 2019-05

The German standard DIN SPEC 27072 (published 05-2019) [80], from the “Deutsches Institut für Normung e. V.” (DIN) defines some mandatory security requirements for IoT devices which are targeted for the consumer market. The standard is called “Informationstechnik – IoT-fähige Geräte – Mindestanforderungen zur Informationssicherheit" in German and "Information Technology — IoT capable devices — Minimum requirements for Information security" in English. It consists of 37 provisions, where 25 are mandatory. The standard is voluntary and does not have to be implemented by every IoT device that is sold on the German market.

The standard should provide a minimum level of cybersecurity and consists of only basic requirements, like secure passwords, etc. (see chapter 3.1.2). In the future, an advanced level standard is planed. This extended standard should be developed in cooperation with the EU, as several countries are interested in it or already started working.

3.1.1 Scope

The DIN SPEC 27072 is mainly for consumer devices in the home environment or small businesses. The scope is limited to the device and not the whole IoT ecosystem (like the cloud or applications for the smartphone). The definition for IoT is restricted to devices which can communicate over IP. This limitation ensures a certain amount of computing power, that encryption and communication requirements can be declared as mandatory.

3.1.2 Content

The 37 provisions can be structured in passwords, cryptography, data, configuration, authentication, update and other. This structure was developed for the presentation at buildingIoT 2020 [11] and uses the contents of the standard [80].

Passwords: No default passwords for all devices are allowed. An individual passwords for each devices should be set or the user should define one. The user-selected password must not be the same as the default password. Regarding of this decision, the user should be able to change all passwords.

When using a remote interface, a sufficient strength of the password is necessary. For example, this can be done by applying the BSI TR-02102-1 [81]. If necessary, a two-factor authentication is recommend (not mandatory).

Cryptography: The cryptography should be developed according to the state of the art. This can be done by using the BSI TR-02102-1 [81] and TR-02102-2 [82]. For development, common and well tested libraries should be used or, in case of an own development of libraries, the implementations should be tested. Keys and other cryptographical material should be stored in protected memory areas. The generation of random numbers should be done according to their security requirements.

One important, but difficult topic is the “crypto-agility”. This enables a device to switch to another cryptographic primitives and / or algorithms. This is a great advantage for devices with a long life span, as it allows them to communicate securely in the future. However, the “crypto-agility” involves a great deal of effort and is difficult to install, especially with low-cost IoT devices. Because of this, it is only recommended to install “crypto-agility” if possible.

Data: The factory reset mechanism should resets all individual data (also keys, etc.). If the user has a possibility to input data, it should be validated every time, regardless if it is only a single value. The data traffic can be encrypted (e.g., with TLS), if it contains passwords or user data, the encryption is required. The integrity and authenticity of communications with a critical function module via remote must be ensured. The definition of a critical function module can be found in the standard.

Configuration: The configuration should only be changed with login. The configuration of other devices (e.g., a router) only by the user. All online functions, which are not necessary for commissioning, should be deactivated and the access to system resources by function modules is restricted.

Authentication: To secure the access, some functions should be only accessible after authentication: the remote access, critical modules and sensitive system information (e.g., configuration). Furthermore, the authentication process should be secured with individual keys for pairing and authentication, and mechanisms against brute force and man-in-the-middle attacks should be implemented.

Update: The possibility for updates, an automatically check per default setting and authenticity and integrity checks of the updates should be implemented. There should be no symmetrical key for all devices and the manufacturer should provide how long the device is supplied with updates.

Other: The model designation should be clearly identifiable and there should be a possibility to check the integrity and authenticity of the security relevant part of the device logic at device startup. In case of a violation, the user should be informed.

3.1.3 Evaluation

The DIN SPEC 27072 is only for consumer devices capable of IP communication. But despite this restriction, it can be used as a good guideline for the development of all kind of IoT devices. All the requirements help to prevent basic security problems and thus, to produce devices with less vulnerabilities.

Due to the narrow scope, there are no requirements for constrained devices (see chapter 6.7.3 for a definition). The whole IoT infrastructure is also not included.

3.2 ETSI EN 303 645

The European Standard (EN) 303 645 [83] from the European Telecommunications Standards Institute (ETSI) is released as version 2.1.1 in June 2020. It is called "Cyber Security for Consumer Internet of Things: Baseline Requirements" and "[...] specifies high-level security and data protection provisions for consumer IoT devices that are connected to network infrastructure (such as the Internet or home network) and their interactions with associated services." [83, p. 6].

Similar to the DIN SPEC 27072, the EN 303 645 provides regulations for consumer IoT devices. But in the case of the EN standard, it includes more devices and more provisions. The IoT devices are not restricted to IP communication capable ones. Constrained devices with low computation power or other restrictions are not able to fulfil every provision. In this case, a justification shall be recorded and the device can still meet the standard.

In order to test the standard, the Technical Specification (TS) 103 701 "CYBER; Cybersecurity assessment for consumer IoT products" [84] is released. This TS contains a methodology to asses all provisions of the EN 303 645 standard.

3.2.1 Scope

The target devices of the standard are consumer devices which are connected to a network structure. They do not have to be connected to the Internet, a connection to a local network is sufficient. There is no other restriction and in addition, the services which are offered for the device are also in scope.

The following devices are given as examples [83, p. 6]:

- connected children's toys and baby monitors
- connected safety-relevant products such as smoke detectors and door locks

- smart cameras, TVs and speakers
- wearable health trackers
- connected home automation and alarm systems
- connected appliances (e.g., washing machines, fridges)
- smart home assistants

The consumer is defined as a “natural person who is acting for purposes that are outside her/his trade, business, craft or profession” [83, p. 9] and a consumer IoT device as a “network-connected (and network-connectable) device that has relationships to associated services and [is] used by the consumer typically in the home or as electronic [wearable]” [83, p. 9].

3.2.2 Content

The standard includes baseline security recommendations, like no universal default password, software updates, input validation, the secure storage of credentials and security-sensitive data, the communication, software integrity, the protection of personal data, etc. Particularly noteworthy are important points that bring great added value and are often overlooked. These are the deletion of personal data, installation and maintenance of devices as well as the security management.

An overview of all the provision topics [83]:

- No universal default passwords
- Implement a means to manage reports of vulnerabilities
- Keep software updated
- Securely store credentials and security-sensitive data
- Communicate securely
- Minimize exposed attack surfaces
- Ensure software integrity
- Ensure that personal data is protected
- Make systems resilient to outages
- Examine system telemetry data
- Make it easy for consumers to delete personal data
- Make installation and maintenance of devices easy
- Validate input data

Every topic contains one or more provision which can be mandatory or optional and act as a guideline. The provisions are extended with examples and the reason they exist. These additional information not only provide a better understanding, but also make it possible to use the standard as an aid or checklist for the development of new devices.

3.2.3 Evaluation

EN 303 645 goes further than DIN SPEC 27072 due to its broader focus and higher number of provisions, making it even better suited to encourage IoT device manufacturers to improve cybersecurity. As the EU standard is weighted higher than a national standard, EN 303 645 will replace DIN SPEC 27072.

A disadvantage of the ETSI standard is the restriction of some provisions as a recommendation. This means that not every point has to be implemented by the manufacturer. Furthermore, there is the possibility that a manufacturer marks his device as a restricted device and thus, a justification is sufficient to not have to implement provisions.

3.3 The Radio Equipment Directive

The legal act of the European Union, the directive 2014/53/EU [85], is called Radio Equipment Directive (RED). Requirements and regulations for all kind of radio equipment are developed to ensure the security and operability between devices. The legal act is intended to ensure that the directives are harmonized in the EU.

In the regulation of 29.10.2021, for example, the focus is on networked children's toys, in addition to general IoT devices. The focus in this regulation is the protection of the network, as well as the protection of personal data and the privacy of the user [86].

The directive is to be seen as very positive, as the security for IoT devices is increased and the individual states of the EU are obliged to implement it. This means that manufacturers must comply with certain standards, but do not need to evaluate them individually for each market. The initial approaches are promising, but concrete conditions are currently still in development.

3.4 The Common Criteria for Information Technology Security Evaluation

The Common Criteria for Information Technology Security Evaluation (short Common Criteria or just CC), is an international standard to evaluate the security of IT solutions, where users can define security targets and vendors can claim that their product meet these targets. A third-party (e.g., testing lab) can prove this claims and evaluate them in a standardised way. The evaluation methodology is described in the Common Methodology for Information Technology Security Evaluation [87].

The CC is defined in ISO / IEC 15408 [88] and widely used in the whole world. Therefore, it is accepted and commonly known as a security measurement. But the downsides of CC are the complexity and its large scale. The CC is split into three parts, the first part (introduction and general model) consists of 106 pages [89], the second part (security functional components) 323 pages [90] and the third part (security assurance components) of 247 pages [91] in the current Version 3.1 Revision 5. For a whole IoT environment, the CC is very complex to use, even for large device manufacturers. However, designations and definitions can be derived from the CC which are used in other standards.

The CC is not a binding requirement for IoT devices, but manufacturers can create a security assessment in accordance with the CC. For the development of special IoT standards, the CC can be used as an assistance, but should not be adopted to a large extent due to its complexity.

3.5 The EU Cybersecurity Act

The EU Cybersecurity Act (Regulation (EU) 2019/881 [92]) strengthens the ENISA and in particular promotes the development of cybersecurity certifications with the help of ENISA [93]. The goal is to establish a European cybersecurity certification framework [94] to improve the cybersecurity of information and communications technology products.

This means, in addition to the standard developing organizations CEN, CENELEC and ETSI, a further organization has been commissioned to develop basic standards for the IoT sector. ENISA should cooperate with the other organizations and place particular focus on horizontal standards. These standards should cover as many devices as possible and give baseline requirements.

As standardization offers a good opportunity to ensure a higher level of security, the Cybersecurity Act can be regarded as positive. The focus on horizontal standards is well chosen as it limits the number of standards as they apply to many devices and thus, manufacturers are not overrun with new standards. The standards are intended to cover information and communications technology products, but no restriction or categorization of IoT devices is yet available.

3.6 General Data Protection Regulation

The General Data Protection Regulation (EU) 2016/679, short GDPR, is an official regulation in the European Union. It aims to protect the personal data of natural persons in relation to data processing [95]. As in many IoT devices, personal data is processed, it must also be applied by IoT manufacturers.

Article 5 of the GDPR describes the "principles relating to processing of personal data" as follows:

"Personal data shall be:
(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or

organisational measures ('integrity and confidentiality')."
(GDPR - Article 5 - L 119/35 [95])

The first sections (a to e) concern the data which should be stored as sparingly as possible and only for a necessary purpose. Section f deals with security. It must be ensured that the data is protected against modification or loss. But concrete measures are not specified. It is only required that the appropriate measures be taken depending on the risk.

The GDPR, regardless of their privacy scope, is a good improvement to help the IoT sector get more secure. If private data is processes, there must be security requirements in the complete process. Certain weaknesses are the loose definitions, as Article 5 (f) only states: "using appropriate technical or organisational measures" [95].

3.7 NISTIR 8259

The National Institute of Standards and Technology (NIST) from the U.S. Department of Commerce released in 2020 recommendations for IoT manufacturers in their publication NISTIR 8259 "Foundational Cybersecurity Activities for IoT Device Manufacturers" [96]. The publication is focused on newly developed devices, but can also be used on existing ones.

"The IoT devices in scope for this publication have at least one transducer (sensor or actuator) for interacting directly with the physical world and at least one network interface (e.g., Ethernet, Wi-Fi, Bluetooth, Long- Term Evolution [LTE], Zigbee, Ultra-Wideband [UWB]) for interfacing with the digital world. The IoT devices in scope for this publication can function on their own, although they may be dependent on specific other devices (e.g., an IoT hub) or systems (e.g., a cloud) for some functionality." [96, p. iv].

This definition is similar to the ISO/IEC 20924:2018 definition (see chapter 1.1.1), as the IoT device requires a network interface and an interaction with the physical world.

In contrast to DIN SPEC 270072 and ETSI EN 303 645, the content of NISTIR 8259 does not consist of provisions, but describes a procedure in six activities [96, pp. v–vi]:

- Activity 1: Identify expected customers and users, and define expected use cases.
- Activity 2: Research customer cybersecurity needs and goals.
- Activity 3: Determine how to address customer needs and goals.

- Activity 4: Plan for adequate support of customer needs and goals.
- Activity 5: Define approaches for communicating to customers.
- Activity 6: Decide what to communicate to customers and how to communicate it.

(NISTIR 8259 [96, pp. v–vi])

The activities do not contain concrete measures, but rather hints for finding the appropriate measures based on the goals. For example, under activity 3 is the consideration: "How strongly an entity's identity needs to be authenticated before granting access if the entity is a human (e.g., PIN, password, passphrase, two-factor authentication) or system/device (e.g., API keys, certificates)" [96, p. 13].

In summary, these are recommendations which are intended to encourage the manufacturer to improve security with certain measures at his own discretion, based on a target analysis.

As seen here, there are also efforts in the U.S. market to increase cybersecurity in IoT. The NISTIR 8259 is a good start and provides useful guidance for the development of new IoT devices. It is not a mandatory standard and it does not include specific measures. The publication only improves IT security for manufacturers who are already considering it and are looking for assistance.

3.8 Regulatory proposal of the UK Government

On January 28th, 2020, the UK Government announced a regulatory proposal for consumer IoT devices for cybersecurity [97]. They focus on three aspects from the ETSI Technical Specification (TS) 103 645, which is an early draft of the ETSI EN 303 645 [97, pp. 17–20]:

- IoT device passwords must be unique and not resettable to any universal factory setting.
- Manufacturers of IoT products provide a public point of contact as part of a vulnerability disclosure policy.
- Manufacturers of IoT products explicitly state the minimum length of time for which the device will receive security updates.

(Government response to the Regulatory proposals for consumer Internet of Things (IoT) security consultation [97, pp. 17–20])

With these three rules, the security of consumer IoT devices should increase regarding to botnets and the manufacturers are more willing to implement it, as the requirements are not so extensive.

A regulatory for all products can significant increase the security, but there should be several requirements. Only because an insecure password is the biggest security hole, it is not the only one. At the moment, the regulatory is still in development. Therefore, a more precise assessment is not being carried out at this time.

3.9 Finnish Cybersecurity label

Traficom, the Finnish Transport and Communications Agency, announced a cybersecurity label in 2019, which is based on the ETSI EN 303 645 standard [98]. The label is focused on the consumer market and should help customers to buy secure products. As the contents in the label are similar to the EN 303 645 standard, no additional requirements needed to be considered by IoT manufacturers which already use the standard.

The label states out the importance of standards and even before an international solution is finished, Finland is addressing IoT cybersecurity. The lead by Finland also shows the acceptance of EN 303 645 and means that development here has been in the right direction.

3.10 Evaluation Security Standards

DIN SPEC 27072 only focuses on devices that can handle IP communication, while EN 303 645 covers all devices. Both standards refer to the devices and in the case of the latter, the services are in focus, too, but only a few provisions refer to them. The RED refers to all devices that communicate wirelessly in any way. The Common Criteria can be used for all devices and services, but is not a mandatory requirement. The EU Cybersecurity Act is intended to drive standardization overall, while still driving the missing standards for services, cloud services, etc. The GDPR refers especially to personal data and is a positive step in this direction. The other regulations presented, showing the development in other countries. They mainly refer to the devices as well.

Many concrete standards for the services that come with the IoT devices are missing. An IoT device is designed to communicate with a network, usually the Internet, and therefore, not only the device itself must be considered, but also the further processing of the data. This includes the individual services, cloud services, applications, servers, etc.

For this thesis, the focus is on applicability. Which standards does a manufacturer have to implement, if he wants to launch an IoT device on the market and is there any assistance for the development phase? To answer this question, one needs an overview of which standards are to be applied for a specific device category. But first, the devices have to be classified into the categories. For example, if a manufacturer is developing a device for the consumer market, it is not sufficient to use the consumer category. DIN SPEC 27072 is only applied, if IP communication is also supported. If the device only supports wired communication, the RED does not have to be considered. These difficulties and differences do not make it easy for a manufacturer. Optional standards, which are not mandatory, can be a help in the development and should also be easily found.

3.11 Summary

The standards presented in detail refer to consumer products, but there are also some standards for industrial and enterprise devices. For industrial devices, there is the IEC 62443 series (Industrial communication networks - IT security for networks and systems) [99], which combines several standards for cybersecurity and is much more comprehensive than DIN SPEC 27072 and EN 303 645. A comparison between IEC 62443 and ETSI EN 303 645 shows that there are significantly fewer provisions in the consumer area (263 to 68) and 32 percent of the requirements found in both standards are less detailed and in-depth in EN 303 645 [100]. These results make clear that there is still a lot of potential in the consumer sector. The regulations in the industrial sector cover far-reaching topics such as processes, organizational measures, guidelines or security levels and are not limited to the devices [99]. Not all processes can be implemented in the consumer area, since there is no administrator for the installation and maintenance of the network.

The standards presented are only a selection and several new ones are to be added in the coming years. DIN and DKE have presented a roadmap [101] that specifies which topics will serve as the focus for new standards in Germany in the future: Data protection, energy supply and generation, industrial production (Industry 4.0), health information systems and medical technology, electromobility, smart home. In addition, the new standardization field Ambient Assisted Living (AAL) is emerging. This shows that cybersecurity standardization is still in its infancy and further standards will follow. It does not only refer to German projects, but also to the cooperation at European level with CEN, CENELEC and ETSI.

The U.S. NIST has also published a status report on cybersecurity standardization with NISTIR 8200 [102]. The document provides an overview of the existing standards and identifies the gaps in the field of IoT. It deals with standards for Cryptography, Cyber Incident Management, Hardware Assurance, Identity and Access Management, Information Security Management Systems, IT System Security Evaluation, Network Security, Physical Security, Security Automation and Continuous Monitoring, Software Assurance, Supply Chain Risk Management and System Security Engineering [102, pp. 36–59].

An extended list of IoT standards can be found in chapter 7.1, where the standards are assigned to the individual categories and characteristics.

4 Problem Statement

The problems of IoT in terms of cybersecurity and the possible solutions have been explored in the last chapter. A core problem is the definition of IoT. In this chapter, the problem is identified more precisely, to better understand the solution that is researched within this thesis.

4.1 Problematic Definition of IoT

Because of the broad definitions for IoT and IoT device (see chapter 1.1.1 and chapter 1.1.2), it is difficult to use the terms. Some people are talking about the IoT and only include smart home devices, other people don't use the term IoT with smart home. They consider just industrial sensors and actuators as IoT. There are a lot of definitions and understandings of the IoT. Most of the time, it is not clear which devices are included or not.

Google Scholar returns about 950.000 results for "IoT" [103] and about 3.410.000 results for "Internet of Things" [104]. Only a few extend the research title with additional information about the devices which are in scope. But the publications are covering research about IoT in general, consumer products (smart home), industrial applications, enterprise systems, etc.

In the study of 2020, which is about different categories of IoT in scientific publications [2], six search engines were used to find out how scientific publications use the term IoT. Additionally, one hundred publications were selected and categorized by hand.

The results state out that IoT can be roughly divided into the three categories consumer, enterprise and industrial. Depending on the search engine, almost all publications can be assigned to the individual subareas. The manual evaluation shows that there are also general publications which cover the whole area of IoT, since, for example, new encryption methods can be used in any domain. The distribution of the different categories can be seen in Figure 4.1. The sum can go over one hundred percent, because some publications fit into several categories. If the sum is lower, the publications cannot be assigned exactly by limiting the search with the keywords.

A major problem, shown by the manual evaluation of the publications, is the difficulty of classification. For example, if results on industrial IoT appli-

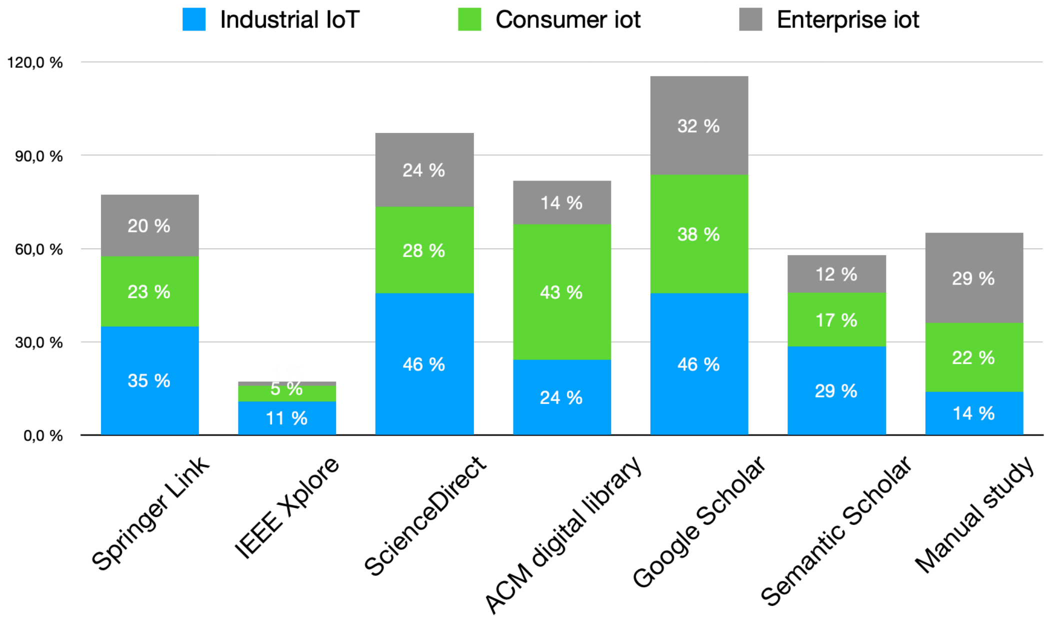


Figure 4.1: IoT in Research Libraries [2]

cations are wanted, the results can be narrowed down using the search terms “industrial” and “iot”. But since a lot of publications do not use “industrial” in the keywords, not all related publications are found. Only in 9 out of 100 cases, one can determine the category with the keywords alone.

As a recommendation, it is better to work with keywords in research, because the category only becomes apparent after reading the abstract or the text in the most cases. General publications can use the term IoT, but more specific research should be provided with a precise categorization to make it easier to find the desired research from all IoT publications.

Standardization organizations suffer from the same problem. At the beginning of an IoT regulation, they have to decide which IoT devices are included. Some use restrictions like consumer devices or industrial devices, others make demands on the devices. There are additional definitions for constrained devices, to include and exclude some of them. These definitions are only valid within the regulation.

In chapter 3.10, the different standards for consumer products are using restrictions to limit the devices which they are applied. For example, the DIN SPEC 27072 is limited to devices using the IP. These inconsistent definitions complicate the work of manufacturers, to find the appropriate standards and regulations for their products.

4.2 Motivation

As seen in chapter 2, a lot of security issues exist in all areas of IoT. Most of them can be avoided by trivial means. Standards for cybersecurity are one solution to address these issues. However, finding the appropriate standard for each IoT device usually requires a detailed analysis.

As mentioned in chapter 4.1, problems of the definition of IoT and the presented cybersecurity standards in chapter 3, a clear categorization for IoT and IoT devices is necessary. The standards use different definitions and for each product, an evaluation of all standards is needed to determine which ones are necessary to observe and apply.

But it is not just the standards that motivate precise categorization. At conferences and in conversation with other scientists, people often do not talk about the same thing when it comes to the IoT.

This motivates to research a model for the IoT which categorize the different areas, to create both, an assignment of devices to the categories, and an assignment of standards to the categories. This allows the standards to be mapped to the devices or vice versa. Chapter 6.2 presents all the precise, measurable objectives of this model.

4.3 Statement

The following short statement summarizes the problem:

There is no scientific model for the IoT which can map the different areas in the sense of cybersecurity standards and research publications.

This statement leads to the fact that in this thesis, a model is researched which fulfills the mentioned requirements. The whole requirements, as well as the evaluation, were scientifically investigated and presented in the course of the research. The objective is to scientifically model the IoT and taking into account its characteristics, conditions and influences.

5 Related Work

There have already been many attempts to divide the IoT world into different categories. Some of them have already gained acceptance or have been subsequently counted as IoT. One example is the smart home which is a separate term that has already evolved from home automation and is now considered as a part of the IoT [20].

In science, there are not many attempts to concretely define the IoT. As a rule, the term is briefly described at the beginning of the publication and thus defined as needed. Some scientific publications often use IoT categories that are taken for granted, but do not describe in detail what is meant by them. Familiar generic terms are used, for example, smart home, smart grid, smart cities, smart healthcare, smart manufacturing, smart transportation [105], smart retail, smart agriculture [106], etc. In the study about different categories of IoT in scientific publications [2], 100 publications were analyzed and no common definition of IoT was found.

In other studies on the IoT, categories are also used which are defined more precisely, but do not follow a uniform rule. Three examples, the World of IoT Sector Map from Beecham Research, a McKinsey Research Report and a Statista Survey, are disccussed in more detail in the following chapters.

In the development of standards, either existing standards are used as a reference or there are strong discussions about what kind of devices the new standard should apply to. With a uniform scheme, these discussions would be eliminated, since a standard is usually intended to apply only to a specific category of devices.

The following chapter provides an overview of other approaches, some of which are considered in more detail, to show the delimitation (chapter 5.3) from this thesis work.

5.1 Overview

In "IT Security of Cloud Services and IoT Devices in Healthcare" [107], the authors described a categorization of medical IoT devices into four distinct risk classes (low risk, medium risk, high risk and very high risk) in their presentation at the conference. They also distinguish between integrated care and homecare. Homecare is aimed at treating patients at home or in nursing homes, while integrated care involves digitalization in medical facilities.

This categorization is helpful because the different risks are considered, which in the health sector, can even have life-threatening effects. Therefore, devices that can harm a person should have a higher safety standard than others. For this thesis, the details in the healthcare sector are not distinguished, because the classification is too complex.

As described in the publication, the following IoT devices are used as an example of Health IoT: hip prosthesis, cardiac catheter, x-ray, infusion pumps, x-ray data, ultrasound, wheelchair, fever thermometer. For each device, the networked variant is meant.

In a publication by Zuerner, the devices are given a label that includes the four categories Use Case, Data Flow, Economy and Lifecycle, and Management and Control. This label is intended to improve the organization of networks (similar to IoTAG, chapter 2.5.1) and ensure transparency regarding social acceptance and regulations [108]. The categories are separated into more possible options. The Use Case category determines which application the device has by looking at the data flow: data exchanged between machines, data sent from machines to humans, data sent from humans to machines or data exchanged between humans. The Data Flow category defines, whether data is sent, received, sent in both directions, or no data is sent at all. The Economy and Lifecycle category consists of the characteristics: date of service, energy requirements and backup mechanisms contained or required. The last category has the three characteristics: no control or management, infrequent or local control, and complex, or frequent control.

J. E. Ibarra-Esquer et al. describe a “Graphical Framework for Categorizing Data Capabilities and Properties of Objects in the IoT” [109]. For this purpose, they use five capabilities to trace the data process. The procedure should provide an insight into the state, communication and data processing of the evaluated device. “Being uniquely and unmistakably identified”, “Being able to know their precise physical location in the world by their own means”, “Obtaining data from the environment or their actual state”, “Acting on the environment or their actual state” and “Processing data obtained by them or received via the Internet” [109] are the capabilities.

E. Siow et al. [110] categorize the different application areas by impact to Society, Environment and Economy. Society contains the three domains Health, Transport and Living, while Economy is mapped to Industry. The different themes and domains contain then areas (e.g., Healthcare, Fitness, Smart Grid) and topics (e.g., Smart City, Smart Building, Smart Home). A more precise assignment to the specific devices does not take place, since the publication focuses on the processed data.

The NISTIR 8200 Status Report [102] classifies its examples into the following five categories: Connected Vehicles, Consumer, Health and Medical Devices, Smart Buildings, and Smart Manufacturing. This classification is for examples only and is not intended to be complete. Since the report looks at the cybersecurity standards, the allocation was deliberately laid out according to the standards and is helpful for the classification in this thesis.

5.2 Examples

Three examples of categorizations are examined in more detail. These are the World of IoT Sector Map from Beecham Research, the MCKinsey Research Report and a Statista Survey. These three were chosen, because they are often cited and used. They try to define the categories more precisely and assign the different devices, which is also the goal of the research in this thesis.

5.2.1 Beecham Research - World of IoT Sector Map

The Beecham Research's World of IoT Sector Map segments the IoT Market into nine sectors [111]:

- Building and Construction
- Energy
- Consumer and Home
- Health and Life Science
- Industrial
- Transport and Logistics
- Retail
- Security and Public Safety
- ICT

These nine sectors are further divided into main application groups with different key applications. For example, Consumer and Home is divided into [111]:

- Infrastructure (key applications: Wiring, Network Access, Energy Management)

- Awareness and Safety (key applications: Security/Alerts, Fire Safety, Environment Safety, Elderly, Children, Power Protection)
- Convenience and Entertainment (key applications: Heating / Climate, Lighting, Appliance, Entertainment)

As a result, the sections include the devices which can be assigned to this category. For example, in the case of Consumer and Home, a video camera is part of the application Security/Alerts and assigned accordingly.

5.2.2 McKinsey Research Report

A research report by McKinsey uses the top use cases to classify the environments for the IoT [27, p. 16]:

- Factories
- Human Health
- Work Sites
- City
- Retail Environments
- Outside
- Home
- Vehicles
- Offices

This type of classification is well suited to show the individual markets and their importance. The growth can be shown depending on the environment and the different percentage increase can be seen.

5.2.3 Statista Survey

In a survey from Statista on the number of IoT devices, the following sectors for categorization are used [24]:

- Agriculture, Forestry and Fishing
- Mining and Quarrying
- Manufacturing
- Electricity, Gas, Steam and A/C

- Water Supply and Waste Management
- Construction
- Retail and Wholesale
- Transportation and Storage
- Accommodation and Food Service
- Information and Communication
- Finance and Insurance
- Professional, Scientific and Technical
- Administrative
- Government
- Health and Social Care
- Arts and Entertainment

These sectors are very detailed which is important for a survey of this scope to be able to evaluate the details for each sector. There are too many sectors for a general categorization which is visible in the proportion of the small sectors with less than one percent share (Agriculture, Forestry and Fishing 0.2 %, Mining and Quarrying 0.2 %, Construction 0.1 %, Accommodation and Food Service 0.7 %, Information and Communication <0.1 %, Finance and Insurance 0.5 %, Professional, Scientific and Technical <0.1 %, Health and Social Care 0.4 %, Arts and Entertainment <0.1 %) [24].

5.3 Delimitation

The scientific publications are not suitable for categorization, because no classification goes far enough and defines clear categories. The terms used are often precisely defined, but this is done depending on the publication and thus, too many different definitions are created.

The World of IoT Sector Map from Beecham Research is very detailed and every device can be found in the categorization. There is no proof whether it is really possible to find a category for every device, but this can be assumed due to the fine-grained division. This categorization is perfect for the assignment to the different sectors, but too detailed for the cybersecurity standards shown in chapter 3, as they do not, for example, distinguish between retail and building. The Transport and Logistics sector contains both, the cars and trucks as IoT devices, as well as the hardware for the warehouse, etc. This means that the different standards cannot be applied to all devices in this sector. Standards for connected cars, which are designed for safety, do not have to be applied to warehouse management.

The McKinsey Research Report is designed for the different markets from a financial perspective and therefore, the categories are also not suitable for the cybersecurity standards. Factories, Work Sites, Outside and Offices are too close together in the kind of IoT devices. One device can be part of all the named environments, but a standard is responsible for the device, regarding of the use case.

The categorization of the Statista Survey is, as already mentioned, too detailed in some areas, which also becomes apparent when some categories are combined. The type of devices and the security level remain the same. For example, it is possible to combine “Electricity, Gas, Steam and A/C” and “Water Supply and Waste Management”. The common category now includes critical infrastructures which have the same regulations.

Existing standards for cybersecurity also use a categorization, since they are only responsible for certain areas. The standards presented in chapter 3 are mostly assigned to the consumer area. This categorization is used as the basis for the model in this thesis, since an objective of the model is a mapping for IoT devices and cybersecurity standards (see chapter 6.2) and there is currently no standard for this categorization.

5.4 Summary

Since the categorization for the security standards do not yet have a firmly defined scheme and there is no scientific solution, a model is researched in this thesis. The existing categories in this chapter will be used as a guide and will be included in the final evaluation in chapter 7.3.

6 Internet of Things Model

This chapter describes the researched model in detail and proves its applicability to all IoT devices, as well as, to prevailing cybersecurity standards.

For this purpose, existing, established terms are used and objectives of the model are defined in advance. Subsequently, the developed categories, additional characteristics, architectures, components, devices, characteristics of the devices and the limitations of constrained devices are described. This is followed by an explanation of how this model can be applied.

6.1 Usage of Existing Categorizations

Already known and established categories and classifications are adopted for the categorization in this model. In this chapter, all the used existing categorizations are pointed out.

The study, "A Study about the Different Categories of IoT in Scientific Publications" [2] has shown, that all publications which are not device-unspecific, can be assigned to the three categories consumer, enterprise and industrial. Some of these categories are already established, e.g., smart home as a category for consumer products. Therefore, these three categories are used for the first classification.

6.1.1 Single Use and Platform Devices

Smartphones, personal computers, workstations, etc. are platform devices. These devices can be extended with software to fulfill many use cases. In some considerations, the basic IoT device is not a platform device, because it is less complex and only has one use case (single use).

This distinction has some disadvantages: the devices are getting more complex and typical IoT devices can be considered as platform devices. For example, both, a smart TV and a smart assistant with a display, can be extended with additional software and new use cases. Another definition describes single use devices as devices, where the software is completely under the responsibility of the manufacturer and platform devices, where it is possible to install third-party software (this definition was used in the CEN working group JTC13/WG6 and was not developed as part of this thesis).

In this work, the second definition is partly used to describe a complex device (see chapter 6.7.1). The focus relies on third-party software, as the manufacturer is not the only one responsible for security.

6.1.2 Constrained Devices

The "Security and Resilience of Smart Home Environments" study from Enisa includes a distinction between constrained devices and high-capacity devices. Constrained devices are classified from class 0 to 3, depending on their RAM capacity, memory storage capacity and CPU power [73, pp. 13–14]. This classification depends on a fixed value and would thus have to be constantly updated. Therefore, the dependencies are used, but defined differently (see chapter 6.9).

6.2 Objectives

One scheme, for all IoT devices, architectures and different definitions is the outcome of this model for the IoT. The four objectives are to be achieved with the approach:

- New standards can define which IoT category and which devices are covered.
- An IoT manufacturer can categorize its devices and assign them to the appropriate, existing cybersecurity standards.
- Constrained devices can be identified.
- Defined architectures can be assigned to every device.

To reach this objectives, these requirements are necessary:

- Clear and consistent definitions for all parts of the IoT.
- Clarification of the different kinds of constrained devices.
- Every device can be assigned.
- Different characteristics can be assigned.

The objectives can be measured by:

- Assigning a large number of devices to the model, to prove the suitability for every device.

- Assigning the existing cybersecurity regulations and standards to the model.

The first objective cannot be measured, but it should help the development of new standards. It can be verified by mapping the plans for standards (e.g., The Radio Equipment Directive and the EU Cybersecurity Act) to the categories.

The second objective can be measured by assigning a large number of devices to the categorization, to prove that every possible device can be assigned to one category. Some types of devices can also belong to several categories, depending on the specific target group. For example, a temperature sensor can be used in a smart home or in a production hall. In this case, the manufacturer can categorize it according to the desired market, to get a unique categorization.

Also for the second objective, all the cybersecurity standards for the IoT can be assigned to the categories and characteristics. After the classification of the device, it is clear which standards apply to the device. This can be measured by assigning the cybersecurity regulations and standards to the categorization.

The third objective is clearly defined: a constrained device can be identified. In this case, all the necessary limitations are defined. The necessity arises from existing and planned standards.

The last objective refers to the architectures which can also be assigned to each device. This objective can be measured equivalently to the second objective, by assigning a large number of devices to the architectures.

The requirements ensure that the objectives are achieved. This means that the objectives are the desired outcome and the categorization must meet the requirements to achieve the objectives. Each part of the IoT should be clearly and consistently defined. The different limitations of the constrained devices should be clear. Each device must be assignable and further characteristics must be possible, in order not to make the categorization too complex.

6.3 Categories

In the first step, the general IoT category is set:

CIoT	Consumer Internet of Things
EIoT	Enterprise Internet of Things
IIoT	Industrial Internet of Things

IoT should be divided into Consumer, Enterprise and Industrial IoT. These categories were chosen, because some of the terms are already in use and they are all providing a clear understanding as described in chapter 6.1. The following subchapters 6.3.1, 6.3.2 and 6.3.3 define the exact definitions.

Smart home is considered as a part of the category CIoT. Smart grid and vehicles can be assigned to EIoT, but additional requirements are necessary which are not covered in this thesis. Smart grid is a critical infrastructure with its own regulations and vehicles, like connected cars, airplanes and trains, have a big impact on safety and own regulations, too. They can harm people and should be secured in an advanced way.

Devices for military use are excluded from all categories as they may have their own regulations. They can be assigned to EIoT to support manufacturers in development, as the target group has its own experts for setup and maintenance, but are not part of this work.

6.3.1 Consumer IoT

Consumer IoT (CIoT) describes devices, developed for private consumers (end-users) and small businesses. This category includes small businesses, because they often use consumer products and do not have sufficient knowledge of IT. The devices are not set up, maintained and monitored by an administrator. The term smart home and all associated devices are included. Figure 6.1 shows a generic CCIoT network.

Example devices for CIoT are: smart watch, smartphone, smart TV, temperature sensor, smart assistant, security cam, window sensor, etc.

As seen in Figure 6.1, the devices normally connect over a Gateway to the Internet. Some devices can have a direct connection, but others need an additional Gateway (Hub or Smartphone) because they are using short range wireless technologies like Zigbee or Bluetooth. In the case of Wi-Fi, the Internet Gateway (Home Router) directly offers the wireless interface.

The clear definition of CIoT: Devices, which are developed for private customers or small businesses. It cannot be assumed that a professional will take care of the installation and operation.

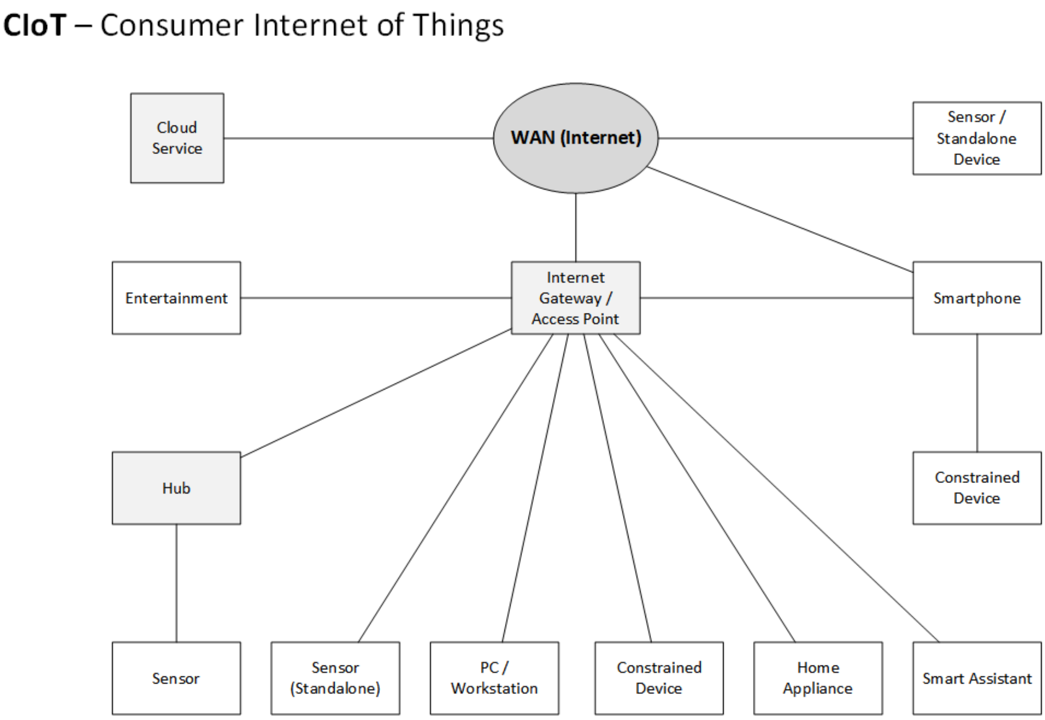


Figure 6.1: Architecture of Consumer IoT

6.3.2 Industrial IoT

Industrial IoT (IIoT) describes the networking of sensors, control units, etc. in an industrial environment. These include devices that produce, control and measure. An exclusion criterion is the use of the equipment in an office environment or in private household. It is closely linked to the notion of Industry 4.0 which is the networking of industrial plants [16]. Industry 4.0 is considered a part of IIoT. The potential for damage is greater in the industrial environment, which is why IoT devices used here are classified in IIoT, rather than EIoT. Figure 6.2 shows a generic IIoT network.

Example devices for IIoT are: production machine, smart farming device, sewage treatment plant machine, wind turbine, lightsensor, safety sensor, pump control, etc.

The network has a simpler structure, but usually a lot more devices (e.g., sensors). In Figure 6.2, it can be seen that the sensors and actuators are connected to a controller. Other devices can also communicate directly with the Internet via the Internet gateway. Edge computing can also be present in IIoT.

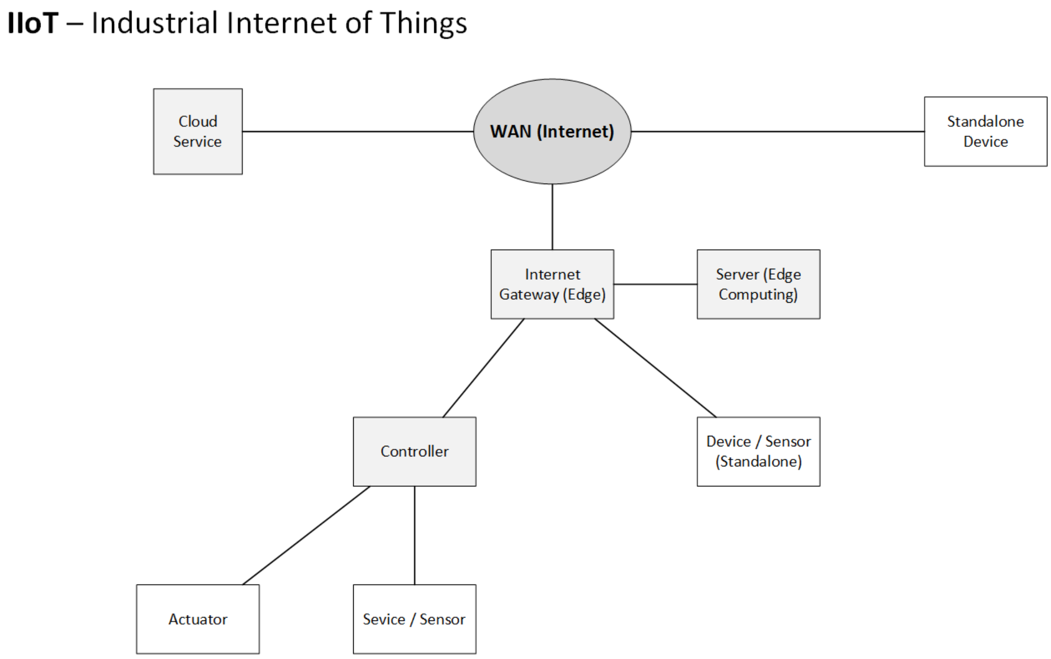


Figure 6.2: Architecture of Industrial IoT

The clear definition of IIoT: Devices, which are used for production or the networking of production sites.

6.3.3 Enterprise IoT

Enterprise IoT (EIoT) refers to all devices used in non-private environments. Excluded are devices that are used for the production or networking of production sites (see chapter 6.3.2 Industrial IoT). Medical devices which are used in hospitals and devices in government environments are included in this category. The key differences between CIoT and EIoT are the installation and maintenance by a professional administrator in EIoT and the higher potential damage that can occur in the case of a failure or impairment in the category EIoT. Figure 6.3 shows a generic EIoT network.

Example devices for EIoT are: security cam, medical operation equipment, cash registers, car charging station, heating control system, etc.

As seen in Figure 6.3, there can be several gateways in the Enterprise category, if the network is divided into different areas. There can also be a local server for services like edge computing. The further connection is similar to CIoT and takes place via switches, access points and finally an Internet gateway.

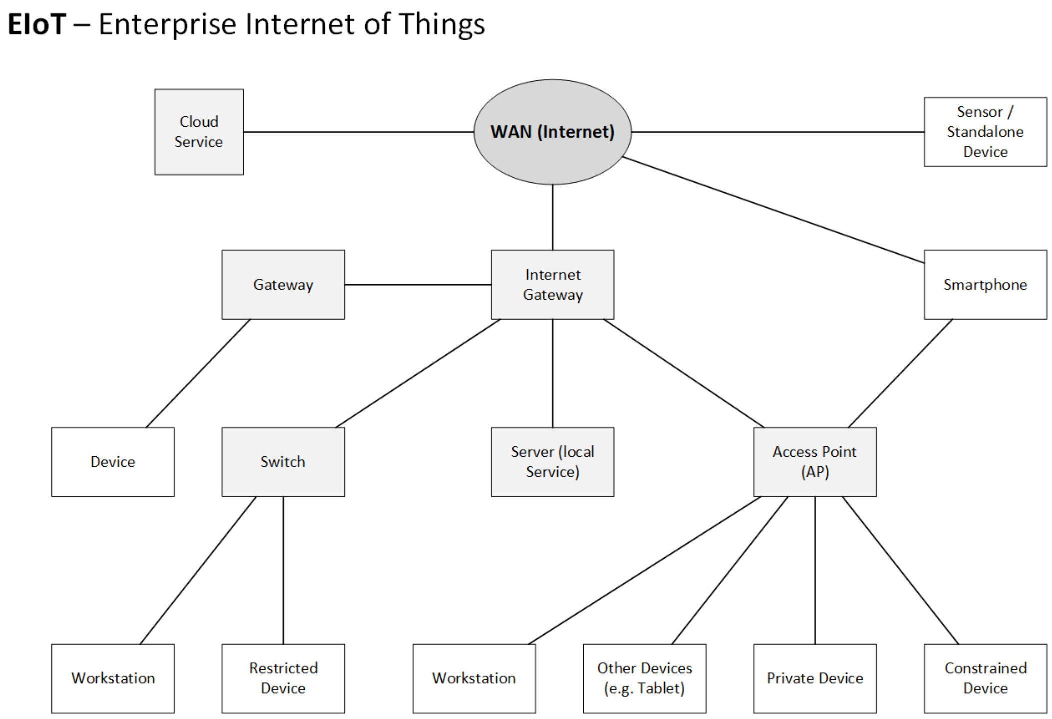


Figure 6.3: Architecture of Enterprise IoT

The clear definition of EIoT: Devices, wich are not in the categories CIoT and IIoT.

6.4 Additional Characteristics of Categories

In addition to the categories, some characteristics may be added. These characteristics extend the regulations and guidelines for the corresponding IoT devices. The characteristics were chosen that the different standards can be mapped.

The possible characteristics are:

CI	Critical Infrastructure
PD	Private Data
SD	Sensitive Data
SY	Safety

In critical infrastructures or in applications which affect the safety of people, it is clear that further regulations are necessary. But also with private or sensitive data, there is more need to protect the device, especially the stored and processed data, from unauthorized access.

A private smartphone always contains private data, but a smartphone used for business does not necessarily have to. In this case, different regulations can be applied for the same type of device, depending on the intended use of the device.

All the additional characteristics are optional. They are used to define the requirements for an IoT device in more detail. In doing so, they differ from other classifications, such as the CIA triad (confidentiality, integrity and availability), because otherwise, no direct mapping to the standards would be possible.

6.4.1 Critical Infrastructure

Services, needed for the society, are called Critical Infrastructure (CI). They provide, for example, supply for electricity, fuel or other services to keep the society running. These CI are important and need extra protection [112]. Categories, extended with this characteristic, have to apply additional regulations.

In Germany, the following organisations or facilities are considered as critical by the BSI: Energy supply, information technology and telecommunications, transport and traffic, health, water, food, finance and insurance, government and administration, media and culture [113, p. 8].

6.4.2 Private Data

Private Data (PD) should not become public and must be subject to special protection (e.g., only accessible with a passphrase). This data includes, for example, personal letters, pictures or contracts.

Private data is the opposite of public data and should only be accessible to the user of the device, or another authorized person [114]. If private data is stored or processed in an IoT device, the requirements for cybersecurity increase and more restricted standards are applied.

If the data is marked as confidential, as defined in ISO/IEC 27000:2018, the characteristic private data applies:

> “property that information is not made available or disclosed to unauthorized individuals, entities, or processes”
> (ISO/IEC 27000:2018, 3.10 [115])

6.4.3 Sensitive Data

Sensitive Data (SD) refers to personal data and data requiring special protection. If this kind of data is processed in the IoT device, this additional characteristic applies.

Personal data contains any data which is related to a person. For example, the name, the date of birth, the age, etc. The GDPR (chapter 3.6) regulates this special protection for personal data and must be applied. The GDPR defines personal data as follows:

> “ ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;”
> (Regulation (EU) 2016/679 - Article 4 (1) [95])

Additionally to personal data, some data requiring special protection, too. For example, data processed in children toys. If a camera is installed in the toy, it should not be possible for this camera to be accessed by unauthorized persons. Therefore, sensitive data contains not only personal data.

6.4.4 Safety

If a device can affect the safety of people or is designed to maintain safety, the characteristic Safety (SY) applies. This applies to the most devices which are related to health, but only if they can affect the safety. For example, medical operation equipment is classified as a safety device, but light-sensors or the smart heating system in a hospital may not harm people and are not classified. Personal heart rate trackers are also no safety devices, because they cannot directly affect the health of a person. But not only health devices can be classified with the characteristic SY, other IoT devices can also be assigned, like production machines in factories.

The IEC 62304:2006 [116] for medical devices can be used to determine if a software can affect the safety. Software safety class B and C can be used as indicators to assign the characteristic to a device:

- Class B: the SOFTWARE SYSTEM can contribute to a HAZARDOUS SITUATION which results in unacceptable RISK after consideration of

RISK CONTROL measures external to the SOFTWARE SYSTEM and the resulting possible HARM is non-SERIOUS INJURY.

- Class C: the SOFTWARE SYSTEM can contribute to a HAZARDOUS SITUATION which results in unacceptable RISK after consideration of RISK CONTROL measures external to the SOFTWARE SYSTEM and the resulting possible HARM is death or SERIOUS INJURY.

(IEC 62304:2006 Medical device software — Software life cycle processes [116])

6.5 Architectures

IoT devices can be connected in different ways to the Internet, respectively to their data processing server. These are the architecture parts or types which occur in all categories:

1. Direct Internet Connection
2. Connection over Internet Gateway (e.g., Router)
3. Connection over a Complex Device (e.g., Smartphone)
4. Connection over a Gateway (out of a separated network)
5. Connection over a Switch / Access Point
6. Connection over a Hub (different kind of connection technology)
7. Connection between Devices
8. Edge Computing

The first connection applies, if the device is directly connected to the Internet. This means, no additional hardware is used between the first public Internet hardware and the IoT device. For example, a connection over a cellular network is used.

Connection 2 uses an Internet Gateway on the IoT device side to establish an Internet connection. Typically, the Gateway is a router.

Connection 3 can include an Internet Gateway, but e.g., on a Smartphone, a direct connection to the Internet is also possible. With this connection type, the IoT device has no direct connection to the Internet or the router.

In connection 4, the data must be transferred to another network. A Gateway (the connection point between the networks) is used for this purpose. This is often applied in companies, when the network is divided into several segments.

Connection 5 uses a switch or an access point for the further transmission of the data. A real-world example would be an IoT device connected to an access point via Wi-Fi.

Connection 6 is similar to type 5, but a different communication technology beside IP communication is used (e.g., Zigbee). In this case, specific regulations, according to the technology, can apply.

Connection 7 uses a different IoT device to establish a connection. This type of connection is also known as mesh networking.

The last type is an addition to the previous connections and occurs when Edge Computing is used outside the IoT device. In this case, an Edge Computing server is located on the IoT device network side.

The different architecture parts are shown in Figure 6.4.

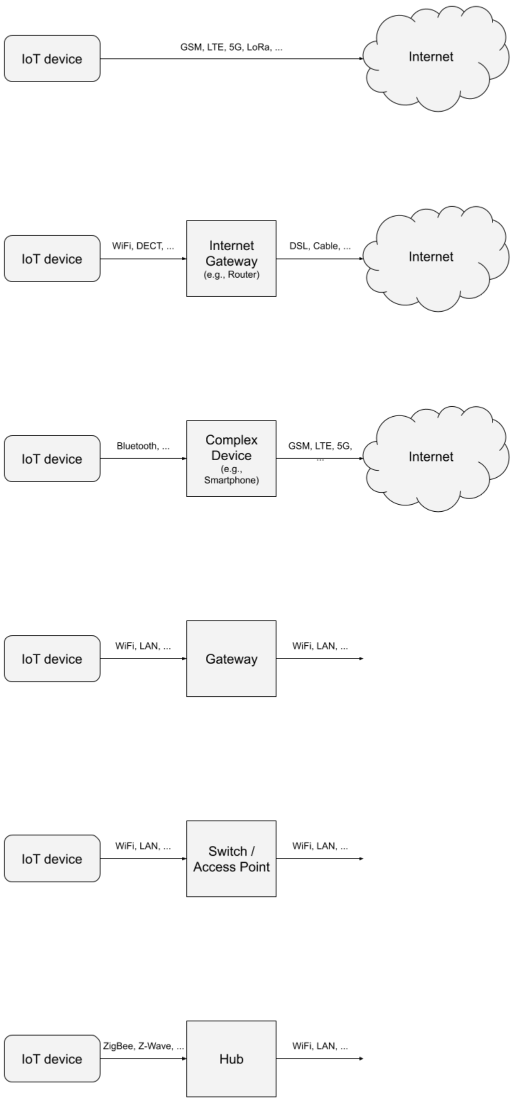


Figure 6.4: Architecture Parts

It is possible to combine these architectures to a given real world scenario. In the example in Figure 6.5, the IoT device is connected over a connection technology like ZigBee, Z-Wave or similar to a hub, which then processes the data over Local Area Network (LAN) to a Gateway. Between the Gateway and the Hub, an additional Switch is located. The Gateway can be used to separate different networks (e.g., one network for IoT devices and one for workstations). After the gateway, the connections continues over LAN to a router (Internet

Gateway) and finally, the Internet, respectively the remote data-processing server.

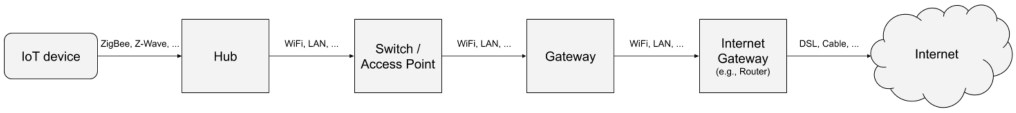


Figure 6.5: Example Combination

Edge Computing is not shown in Figure 6.4, because it can be located anywhere in the local (or remote) network. In the example above, an edge computing device could be added at any point between the IoT device and the Internet Gateway. Normally, the Edge Computing server is not the end-point, because the pre-calculated data is transferred to a remote location for further processing and analysing.

An overview of the three main categories with the generic example architectures is shown in Figure 6.6. A larger version of the figure can be found in the appendix 11.2.

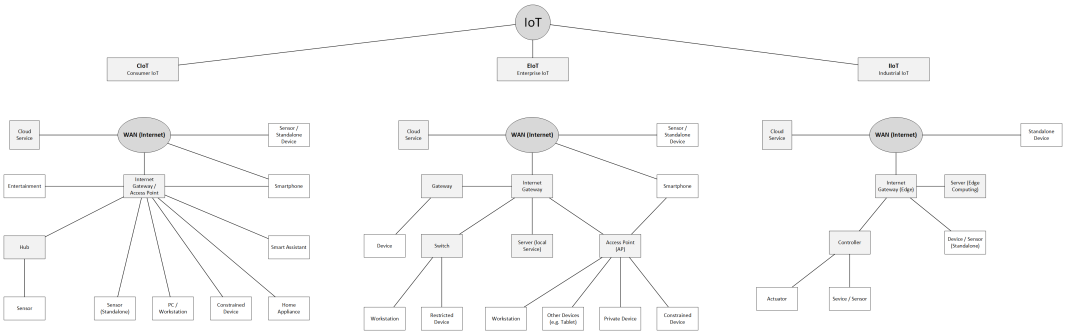


Figure 6.6: Architecture of Categories

6.6 Architecture Components

Architecture components are not directly IoT devices, but needed for the IoT infrastructure. The following components are used to work in an IoT environment:

- Internet Gateway (e.g., Router)
- Gateway, to separate internal networks

- Switch / Access Point
- Local Server / Edge Computing
- Cloud Server
- Application (App)
- Hub (to connect different kind of connection technologies, e.g., Zigbee and Wi-Fi) / Controller (IIoT: to collect data from multiple sensors or control multiple actuators)

As regulations for the architecture components may also be possible, these are also included in the categorization. A router, for example, can also be considered as an IoT device. The technical directive "Secure Broadband Router" (BSI TR-03148 [117]) in Germany specifically concerns a router as an Internet Gateway.

6.7 Devices

IoT consists of different devices with diverse specifications. As the standards and regualtions cannot be applied to every device, it is necessary to categorize them. One category for each different specification (e.g., Bluetooth, Wi-Fi, Zigbee) would be be too much and too confusing, as some devices can occur in several categories. The used solution divides the devices into three categories and then extends them with characteristics (chapter 6.8) and limitations (chapter 6.9). The three categories are:

XD	Complex Device
DD	Default Device
CD	Constrained Device

XD serves as an abbreviation for a Complex Device (e.g., Smartphone, Workstation), DD for a Default Device and CD for a Constrained Device. The limitations from chapter 6.9 are only used with CD.

6.7.1 Complex Device

A Complex Device can be extended by third-party software. The device manufacturer is not solely responsible for the software and, depending on the scope of the third-party applications, security risks can arise. For example, if the configuration is changed or interfaces to the outside are offered. The differentiation to a DD is the ability to load third-party software. This can be application software, as well as, the complete operating system.

Complex devices include smartphones, desktop computers, laptops, smart TVs running Android, etc. In some definitions, they are also called platform devices (see chapter 6.1.1). The exact definition of third-party software can be found in chapter 1.1.9.

6.7.2 Default Device

A Default Device is not a Complex Device and additionally, has no restrictions from Chapter 6.9. This means that the manufacturer supplies the software and no programs from third-parties can be installed.

As a result of the classification, all standards and rules can be applied without restrictions, provided they are valid for the category (chapter 6.3). For example, the following devices are default devices: eBook Reader, Digital Camera, Cash Register.

6.7.3 Constrained Device

A Constrained Device can not always implement all requirements given by security standards. This can be the case because they are constrained by their battery-capacity or they are missing input / output components or other restrictions. They are designed in this way, because it is necessary for the required use case. For example, a small sensor in an industrial production machine. Or, they are constrained, because the manufacturer wants to design them very cost-efficient. To achieve the best security level, the last case should be avoided. As seen in chapter 3.2, the constrained devices are not excluded from certifications like EN 303 645, but they need to document a valid reason.

The definition from EN 303 645 can be used to describe the term:

"device which has physical limitations in either the ability to process data, the ability to communicate data, the ability to store data or the ability to interact with the user, due to restrictions that arise from its intended use" [83, p. 9].

The concrete constraints with further details are described in chapter 6.9.

6.8 Characteristics of Devices

All devices can be extended with characteristics. There are five possible characteristics which are currently useful to map the cybersecurity standards exactly. These characteristics are necessary, because some standards are only applied for wireless communication devices, private devices in the office, etc. For example, the DIN SPEC 27072 (chapter 3.1) only covers devices which are capable of IP communication. Or, devices without a wireless communication interface are not included in the Radio Equipment Directive (chapter 3.3).

There are more characteristics possible, like Wi-Fi-Connection, but at the moment, only these five are necessary to map the existing cybersecurity standards to the different IoT devices. They can be extended at any time, when needed.

An overview over the five characteristics of devices:

1. Private Device (only in EIoT)
2. Trusted Platform Module (TPM)
3. Only cable connection
4. IP-Communication
5. Bluetooth-Communication

Each characteristic can be explained as follows:

1. The characteristic Private Device is only available in the category EIoT. This refers to an employee's personal device that is connected to the corporate network. This is also called "bring-your-own-device".
2. The device has an integrated Trusted Platform Module.
3. The device does not have any wireless interface and therefore, only a cable connection.
4. The device communicates via the Internet Protocol (IP) standard (not exclusive).
5. The device communicates via the Bluetooth standard (not exclusive).

6.9 Limitations of Constrained Devices

Constrained devices can be specified by one or more limitations:

1. Less computing power / no encryption possible
2. Restricted Battery

3. Restricted Memory
4. Restricted Bandwidth (Data Rate)
5. Limited Output
6. Limited Input

Since the limitations are difficult to define, examples are given. Limitations always occur when one required function cannot be fulfilled due to the nature of the device.

1. Less computing power / no encryption possible: The computing power is not sufficient enough to encrypt data or calculate hash values to validate data. As asymmetric encryption is more complex to calculate, a device is not constrained, if it only uses symmetric encryption and can still meet all requirements.

2. Restricted Battery: Some devices need to be small or operate in an environment where it is not possible to change the battery easily. In this case, the devices are restricted by the battery, if they cannot perform encryption, updates or other security related functions in a normal way.

3. Restricted Memory: The memory is restricted, if it is not possible to install (firmware) updates without hardware access or no cryptographic key can be stored on it.

4. Restricted Bandwidth (Data Rate): Depending on the type of communication, the data rate is too slow, if no encryption is possible, because it would take too long to send (or receive) the data for the required use case. This restriction can be related to the battery. For example, a light switch with energy harvesting can just send a short signal.

5. Limited Output: The first connection (pairing) is typically used to exchange a secret (key) for the further secured connections. To ensure that the connection is established with the desired device and not an attacker, e.g., with Bluetooth, a six digit decimal number must be compared on both devices [71]. If it is not possible to show this number, this limitation applies.

6. Limited Input: The same as for the output also applies to the input. In an extended secure pairing process, a code must be entered on a device.

These restrictions were chosen, because, depending on the standard, one restriction already means that a standard does not have to or cannot be applied. For example, as seen in chapter 3.1, the DIN SPEC 27072 is only applicable for devices which are able to communicate via IP. This also excludes devices where no encryption is possible.

6.10 Categorizing

With the categories, the characteristics and the restrictions, every IoT device can be classified. In this chapter, the three IoT devices Smart TV, Traffic Lights and Networked Baking Oven are mapped to the model.

The Smart TV is produced for the end-user market and therefore in the CIoT category. As the TV can save (and possibly pass on) the user's settings and habits, it is given the additional characteristic PD (Private Data). A Smart TV usually connects to the Internet router and afterwards to the Internet. In this case, it uses the architecture 2. If the device is intended to be used in another architecture, it should get another number. This must be determined depending on the specific device and cannot be determined for all smart TVs in general. The TV is no Architecture Component, like a switch or router, so no assignment takes place here. The Device Type can be DD or XD, depending on the running software. If it can be extended with third-party software, it is a XD, otherwise a DD. In this case, additional software can be installed, but only from the manufacturer. It is classified as DD, because the manufacturer alone is responsible for the configuration and security of the device, since no changes from third-parties can affect the device. Depending on the equipment of the device, characteristics for the device are added. In this example, they are IP- and Bluetooth-Communication. As it is not a CD, no device limitations are present. The complete categorization can be tabulated and is shown in Table 6.1.

Table 6.1: Categorization Examples

	Category	Characteristic	Architectures	Architecture Component	Device Type	Device Characteristics	Device Limitations
Smart TV	CIoT	PD	2		DD	4,5	
Traffic Lights	EIoT	CI,SY	1		DD	4	
Networked Baking Oven	EIoT	SY	2		DD	4	

Traffic Lights are not used by private users and belong to EIoT. They are part of a critical infrastructure (CI) and have an impact on the safety (SY). A possible architecture is a direct connection over 3G to the Internet. In addition, there may be other types of communication, for example, Wi-Fi (IEEE 802.11p) for a direct communication with cars. The device type is DD, as there are no restrictions (because of the fixed power supply). The device characteristic is IP-Communication. The complete categorization is also shown in Table 6.1.

Depending on how the Networked Baking Oven is designed, it may be produced for the end-customer market or for a bakery. If the former is the case, it is assigned to CIoT, otherwise to EIoT. In this example, it belongs to EIoT. Since the oven can cause harm to a human, it gets the Safety (SY) characteristic. It is connected to the Internet via the company network, i.e. via an Internet gateway. As device type, it is classified as DD (without restrictions) and it has the characteristic IP-Communication. As before, the complete categorization is shown in Table 6.1.

With these different examples, the practical application of the categorization model is shown. Other devices can be assigned analogously. Another device, from the same kind, can have a different categorization. For example, an industrial sensor can be connected over cable, BT, Wi-Fi or another technology. In every case, the assignment can be different. The generic mapping process is shown in Figure 6.7.

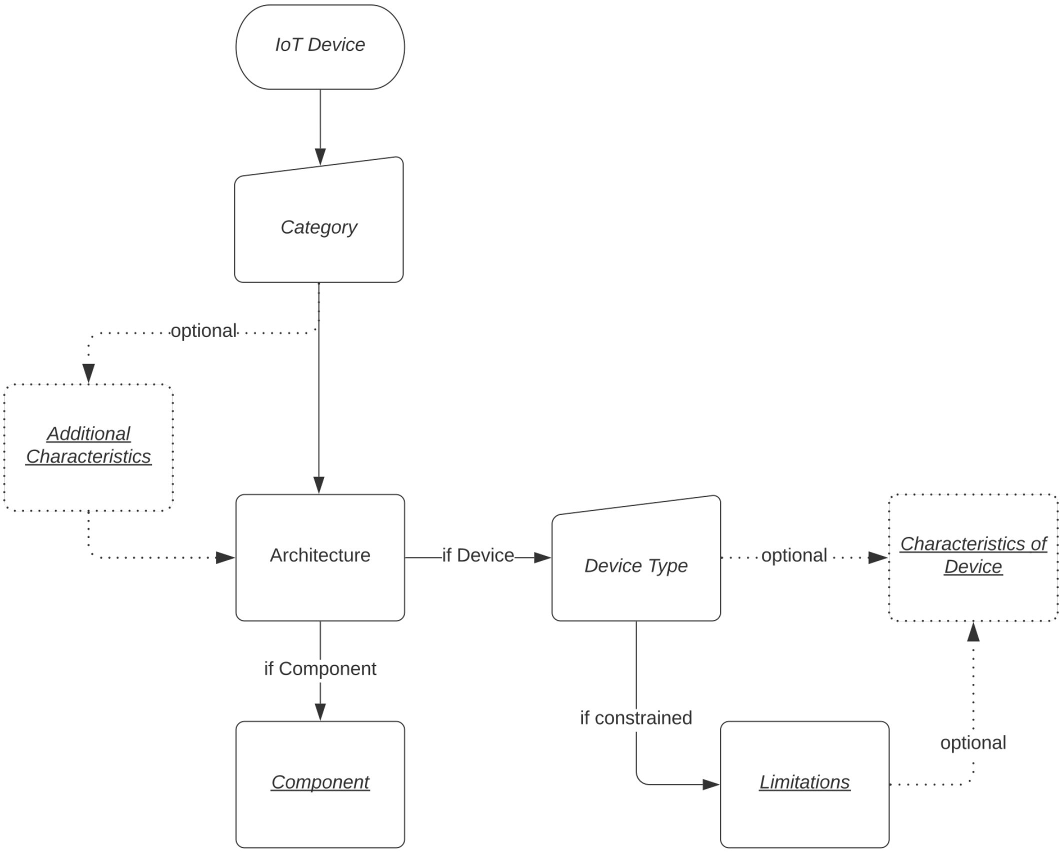


Figure 6.7: Generic Mapping Process

To prove the statement that every devices can be mapped, a large list of devices is mapped. The list is attached in appendix 11.4. If several categories, characteristics, architectures, device types, device characteristics or limitations can apply, they are separated by a comma. Depending on the concrete device, the associated feature must be selected when categorizing a device. If some of these parameters are given in brackets, it means that they are only optional parameters and do not have to apply. Particularly, the device limitations are often different. With vehicles or smart grid devices, a further categorization of the characteristics etc. can be made. However, these devices must still be considered explicitly due to their speciality (own regulations etc.).

The architecture components are also IoT devices due to the broad definition of IoT and integrated into the categorization. They do not require any further classification in the device type or the device characteristics or limitations.

Additionally, all the IoT examples from chapter 1.3 are mapped in chapter 7.2 in the same way.

7 Mapping

In this chapter, the researched model is mapped to the real IoT world. At first, the Guidelines, Standards and Regulations are assigned, then the IoT Examples presented in the first chapter, and finally, the already existing IoT categories. A mapping use case finishes the chapter.

7.1 Mapping Guidelines, Standards and Regulations

Table 7.1 is mapping the Cybersecurity Guidelines, Standards and Regulations to the corresponding IoT categories and characteristics, as well as the restrictions. Some important and well-known ones have been used, but also smaller ones, to demonstrate the wide range of applications. For example, GRVA-01-17 and GRVA-01-18 are standards for vehicles, but also in the table.

The entries are assigned to the respective category for which the standard was developed. Some entries have no assignment, because they are universal and do not refer to a special type of device. But they can be assigned to special characteristics (e.g., the ENISA Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures). Restrictions may also be added. They restrict the entry to a specific characteristic of the device (e.g., only Gateways or IP-Communication).

For example, the ETSI EN 303 645 was developed for consumer products and is assigned to the CIoT category. There are no further characteristics or restrictions. DIN SPEC 27072 was also developed for consumer products, but is limited to IP-Communication. In this case, the restriction is added.

The constrained devices and the corresponding restrictions can be used to exclude requirements in the standards for the assessed device. For example, the provisions 5.1-5, 5.3-2 and 5.3-14 in ETSI EN 303 645 [83] are only for non-constrained devices. In this case, it is helpful to determine beforehand whether a device is a constrained device or not. Then, the provisions can be ignored and do not have to be implemented. It is even possible to define the limitations more precisely that not all provisions have to be excluded directly. For example, if a device does not have a screen, it can be a constrained device,

Table 7.1: Categorization of Guidelines, Standards and Regulations

	Full Name	Category	Characteristics	Restrictions
BSI TR-02102-1 [81]	BSI TR-02102-1: ”Cryptographic Mechanisms: Recommendations and Key Lengths” Version: 2021-1	CIoT, EIoT, IIoT	PD, SD, SY	
BSI TR-03148 [118]	BSI TR-03148: ”Secure Broadband Router” Version: 2020 1.1	CIoT		Components: 1
DIN EN 60335-1:2020-08 [119]	Sicherheit elektrischer Geräte für den Hausgebrauch und ähnliche Zwecke - Teil 1: Allgemeine Anforderungen	CIoT	SY	
DIN SPEC 27072 [80]	Informationstechnik - IoT-fähige Geräte - Mindestanforderungen zur Informationssicherheit	CIoT		IP-Communication
EN 62351-3 [120]	Part 3: Communication network and system security - Profiles including TCP/IP	CIoT, EIoT, IIoT		IP-Communication
ENISA Baseline Security Recommendations for IoT [121]	Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures	CIoT, EIoT, IIoT	CI	
ENISA Good practices for IoT and Smart Infrastructures Tool [122]	Good practices for IoT and Smart Infrastructures Tool	CIoT, EIoT, IIoT		
ENISA Good Practices for Security of Internet of Things [123]	Good Practices for Security of Internet of Things in the context of Smart Manufactoring	IIoT		
ENISA Security and Resilience of Smart Home Environments [124]	Security and Resilience of Smart Home Environments	CIoT		
ETSI EN 303 645 [83]	CYBER; Cyber Security for Consumer Internet of Things	CIoT		
ETSI TR 103 304 [125]	CYBER; Personally Identifiable Information (PII) Protection in mobile and cloud services	CIoT, EIoT, IIoT	PD	
ETSI TS 103 458 [126]	CYBER; Application of Attribute Based Encryption (ABE) for PII and personal data protection on IoT devices, WLAN, cloud and mobile services - High level requirements	CIoT, EIoT, IIoT	PD	
GOV UK - Code of Practice for Consumer IoT Security [97]	Code of Practice for Consumer IoT Security	CIoT		
GRVA-01-17 [127]	[Draft] Recommendation on Cyber Security of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 GRVA	EIoT		
GRVA-01-18 [128]	[Draft] Recommendation on Software Updates of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 GRVA	EIoT		
GSMA IoT Security Guidelines [129]	GSMA IoT Security Guidelines and Assessment	CIoT, EIoT, IIoT		
IEC 62443 [130]	Industrial communication networks – Network and system security	IIoT		
IoT Security Assurance Framework [131]	IoT Security Assurance Framework	CIoT, EIoT		
ISO/DIS 31700 [132]	[UNDER DEVELOPMENT] Consumer protection — Privacy by design for consumer goods and services	CIoT		
ISO/IEC 15045-1:2004 [133]	Information technology — Home Electronic System (HES) gateway — Part 1: A residential gateway model for HES	CIoT		Gateway
ISO/IEC 20924:2018 [134]	Information technology — Internet of Things (IoT) — Vocabulary	CIoT, EIoT, IIoT		
ISO/IEC 24767-1:2008 [135]	Information technology — Home network security — Part 1: Security requirements	CIoT		
ISO/IEC 30141:2018 [136]	Internet of Things (loT) — Reference Architecture	CIoT, EIoT, IIoT		
ISO/IEC 30147:2021 [137]	Information technology — Internet of things — Methodology for trustworthiness of IoT system/service	CIoT, EIoT, IIoT		
ISO/IEC CD 24392.2 [138]	[UNDER DEVELOPMENT] Information technology — Security techniques —Security reference model for Industrial Internet Platform (IIP)	IIoT		
ISO/IEC CD 27403 [139]	[UNDER DEVELOPMENT] Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics	CIoT, EIoT		
ISO/IEC DIS 27400 [140]	[UNDER DEVELOPMENT] Cybersecurity — IoT security and privacy — Guidelines	CIoT, EIoT, IIoT		
ISO/IEEE 11073-10418:2014 [141]	Health informatics — Personal health device communication — Part 10418: Device specialization — International Normalized Ratio (INR) monitor	CIoT	PD	Personal Health Devices
NISTIR 8259 [96]	Foundational Cybersecurity Activities for IoT Device Manufacturers	CIoT		
OWASP - IoT Security Guidance [142]	IoT Security Guidance	CIoT, EIoT, IIoT		
Regulation (EU) 2016/679 [95]	General Data Protection Regulation	CIoT, EIoT, IIoT	PD	
SB-327 Information privacy: connected devices [143]	Senate Bill No. 327 CHAPTER 886 TITLE 1.81.26. Security of Connected Devices	CIoT		IP-Communication, Bluetooth-Communication
Secure Design - Best Practice Guide [144]	Secure Design - Best Practice Guide	CIoT, EIoT		
TCG TPM 2.0 Automotive Thin Profile For TPM Family 2.0; Level 0 [145]	TCG TPM 2.0 Automotive Thin Profile For TPM Family 2.0; Level 0	EIoT		

but still be able to communicate in encrypted form. However, the possibility to indicate new updates may then be missing.

The characteristics can also be used in a standard to restrict requirements. For example, if the device does not process personal data, provisions 5.8-1 and 5.8-2 in ETSI EN 303 645 do not need to be implemented.

Some constraints do not refer to constrained devices, but to the device type. For example, ISO/IEC 15045-1:2004 [133] on gateways or ISO/IEEE 11073-10418:2014 [141] on personal health devices. These restrictions are numerous and not defined in a fixed list.

7.2 Mapping IoT Examples

The IoT examples from chapter 1.3 are mapped to prove that all devices from the examples can be assigned. Additionally, it provides several examples for the model. The tables of the individual examples are constructed equivalent to chapter 6.10.

7.2.1 Smart Home

The smart home example from chapter 1.3.1 is categorized in Table 7.2. There are two Architecture Components, the Router and the Smart Control Hub. The other devices are mixed, DD, XD and CD.

Table 7.2: Categorization of Smart Home Example

	Category	Characteristic	Architectures	Architecture Component	Device Type	Device Characteristics	Device Limitations
Smart Assistant	CIoT	PD,SD	2		DD	4,5	
Smart TV	CIoT	PD	2		DD	4,5	
Smart Fridge	CIoT		2		DD	(3),4	
Robot Vacuum Cleaner	CIoT	(PD)	2		DD	4,(5)	
Smartphone	CIoT	PD,SD	1,2		XD	2,4,5	
Desktop Computer	CIoT	PD,SD	2		XD	2,4,5	
Router	CIoT	(PD),(SD)		1			
Smart Control Hub	CIoT	PD,SD		7			
Smart Lightning	CIoT		2,6,7		CD		1,3,6
Smart Lock	CIoT	SD	2,6		CD		2,5
Window Sensor	CIoT		6		CD		1,2,3,4,5,6
Smart Meter	EIoT	CI,PD,SD	6		CD	3	1,2,3

7.2.2 Wearables

The wearables example from chapter 1.3.2 is categorized in Table 7.3.

Table 7.3: Categorization of Wearables Example

	Category	Characteristic	Architectures	Architecture Component	Device Type	Device Characteristics	Device Limitations
Smart Watch	CIoT	PD	2,3		DD	4,5	
Fitness Tracker	CIoT	PD	3		CD	5	4

7.2.3 Automotive

The automotive example from chapter 1.3.3 is categorized in Table 7.4.

Table 7.4: Categorization of Automotive Example

	Category	Characteristic	Architectures	Architecture Component	Device Type	Device Characteristics	Device Limitations
Car	EIoT	CI,PD,SY	1		DD	1,4,5	
GPS Tracker	CIoT	SD	1		DD	4	
Traffic Lights	EIoT	CI,SY	1		DD	4	
Parking Space Sensor	EIoT		1		CD	4	1,2,3,4,5,6

7.2.4 Smart City

The smart city example from chapter 1.3.4 is categorized in Table 7.5.

Table 7.5: Categorization of Smart City Example

	Category	Characteristic	Architectures	Architecture Component	Device Type	Device Characteristics	Device Limitations
Garbage Can Sensor	EIoT		1		CD	4	1,2,3,4,5,6
Smart Street Lights	EIoT	SY	1		DD	4	
Visitor Counter	EIoT		1,2,6		CD	(4),(5)	1,2,3,4,5,6
Parking Space Sensor	EIoT		1		CD	4	1,2,3,4,5,6
Traffic Lights	EIoT	CI,SY	1		DD	1,2	

7.2.5 Health

The health example from chapter 1.3.5 is categorized in Table 7.6.

Table 7.6: Categorization of Health Example

	Category	Characteristic	Architectures	Architecture Component	Device Type	Device Characteristics	Device Limitations
Heart Pacemaker	CIoT	PD,SD,SY	3,6		CD	(5)	1,2,3,4,5,6
Fall Sensor	CIoT	S	2		CD	4	2,3
Insulin Pump	CIoT	PD,SD,SY	3,6		CD	(5)	1,2,3,4,5,6
Blood Glucose Meter	CIoT	PD,SD,SY	3,6		CD	(5)	1,2,3,4,5,6
Medical Monitoring Device	EIoT	PD, SY	4		DD		

7.2.6 Enterprise

The enterprise example from chapter 1.3.6 is categorized in Table 7.7.

Table 7.7: Categorization of Enterprise Example

	Category	Characteristic	Architectures	Architecture Component	Device Type	Device Characteristics	Device Limitations
Networked Baking Oven	EIoT	SY	2		DD	4	
Temperature Sensor	CIoT		2,6		CD	(4),(5)	1,2,3,4,5,6
Smart Lighting	CIoT		2,6		CD		1,2,3,4,5,6
Online Cash Register System	EIoT	SD	2		DD	2,(3),4	
Workstation	EIoT	PD,SD	2		XD	2,(3),4,(5)	

7.2.7 Industrial

The industrial example from chapter 1.3.7 is categorized in Table 7.8.

Table 7.8: Categorization of Industrial Example

	Category	Characteristic	Architectures	Architecture Component	Device Type	Device Characteristics	Device Limitations
Sensors	EIoT	(SD),(SY)	4,6		CD		1,2,3,4,5,6
Networked Machines	EIoT	(SD),(SY)	4,6		CD,DD		1,2,3,4,5,6
Controllers	EIoT	(SD),(SY)	4,6		CD		1,2,3,4,5,6

7.3 Mapping Existing Categories

In chapter 5.2, already existing categories were presented. These categories were not suitable for assigning all devices to security standards. In this chapter, these categories are assigned to the researched model. It can be shown that

Table 7.9: Mapping: Existing Categories - New Categories

Beecham Research World of IoT Sector Map	New Categorization	McKinsey Research Report	New Categorization	Statista Survey	New Categorization
Building and Construction	EIoT	Factories	IIoT	Agriculture, Forestry and Fishing	EIoT
Energy	EIoT	Human Health	CIoT / EIoT	Mining and Quarrying	EIoT
Consumer and Home	CIoT	Work Sites	EIoT	Manufacturing	IIoT
Health and Life Science	CIoT / EIoT	City	EIoT	Electricity, Gas, Steam and A/C	EIoT
Industrial	IIoT	Retail Environments	EIoT	Water Supply and Wast Management	EIoT
Transport and Logistics	EIoT / IIoT	Outside	EIoT	Construction	EIoT
Retail	EIoT	Home	CIoT	Retail and Wholesale	EIoT
Security and Public Safety	EIoT	Vehicles	EIoT	Transportation and Storage	EIoT
ICT	EIoT	Offices	EIoT	Accommodation and Food Service	EIoT
				Information and Communication	CIoT / EIoT
				Finance and Insurance	EIoT
				Professional, Scientific and Technical	EIoT
				Administrative	EIoT
				Government	EIoT
				Health and Social Care	CIoT / EIoT
				Arts and Entertainment	CIoT / EIoT

the new model could replace the previous approaches. Some categories can be assigned directly, such as Building and Construtction to EIoT or Manufacturing to IIoT. Other categories span multiple areas. Transport and Logistics from the World of IoT Sector Map, includes devices from EIoT and IIoT. Table 7.9 displays the complete mapping from the existing to the new categories

7.4 Mapping Use Case

An example use case shows the benefit of the model, based on the complete process. An appliance manufacturer is developing a new IoT product for the consumer market. The device is intended to make an existing refrigerator “intelligent” by means of a camera and voice recognition. The hardware is integrated into an existing device and a cloud environment with applications is implemented. In order for cybersecurity to be considered at the product development stage, the researched model helps to find the standards and guidelines needed.

First, the target market is determined. In this case, the product is intended for consumers, so CIoT is the category.

Then, the additional characteristics are determined. Due to the fact that a camera and a microphone are used for voice recognition, private data can be assumed. The consumption behavior based on the image of the refrigerator and the voice commands with possibly unwanted sound recordings can be considered as personal data. So, the characteristic PD is added.

The next step is to define the architecture. The hardware is to be connected directly to the home router to establish an Internet connection for the services. In this case, architecture 2 is used.

The hardware runs on battery power because upgrading existing devices should be as easy as possible, so it is a Constrained Device (CD) with the restriction “2. Restricted Battery”. Additionally, the characteristic “4. IP-Communication” is added, since it is connected to the router via Wi-Fi and uses IP.

This results in the allocation shown in Table 7.10.

Table 7.10: Use Case: Intelligent Refrigerator

	Category	Characteristic	Architectures	Architecture Component	Device Type	Device Characteristics	Device Limitations
Intelligent Refrigerator	CIoT	PD	2		CD	4	2

After the device has been mapped in the model, the standards can be easily filtered. Table 7.1 from chapter 7.1 can be used for this purpose. The categories are restricted and standards with characteristics and restrictions are only selected, if they apply. The whole procedure can be automated as described in chapter 8.5.

8 Evaluation

In this chapter, the researched model is evaluated. The fulfillment of the objectives is checked and the applicability of the model in practice is presented. In further research on the model, a tool is planned which automates the assignments and management. The functions and advantages of the tool are briefly presented, but further development is not part of the thesis.

8.1 Benefits of the Model

As seen in chapter 5, there is no scientific model for cybersecurity standards and the categorisation of IoT devices. No scientific publication provides a classification of IoT devices to the associated standards. Even in standardization and common usage, there are no universal definitions of IoT and the associated devices. The model researched in this thesis thus fills a gap in science and practice. The individual areas of IoT can be distinguished and the different devices can be categorized according to their characteristics.

The model is easy to apply which is illustrated in Chapter 7. A device or standard can be classified according to the defined characteristics. It is possible to implement the modelling in software and automate the process.

The added values are presented in chapter 8.4 and cover many use cases. In science for new publications and in standardization work or conferences, the model provides a clear mapping of the diverse IoT world. The model was designed for flexibility, so it can be adapted and used in the future.

In summary, the following key figures can be listed:

- New model that fills a gap in research
- Applications of the model in practice
- Easy to use
- Can be automated well
- Many future use cases
- Flexibility for future changes

8.2 Fulfillment of Objectives

In chapter 6.2, the objectives were defined and requirements and measurements were derived from them. The fulfillment of these objectives is presented in this chapter. The measurements are checked first, then the requirements and next the objectives are validated.

The two measurements are:

- Assigning a large number of devices to the model, to prove the suitability for every device.
- Assigning the existing cybersecurity regulations and standards to the model.

The first measurement is proven by the mapping of the devices to the model. This can be seen in chapter 7.2 and a more extensive list can be found in the appendix 11.4.

The second measurement is proven by the mapping of the cybersecurity regulations and standards to the model. This can be seen in chapter 7.1.

Next, the requirements are reviewed. The four requirements are:

- Clear and consistent definitions for all parts of the IoT.
- Clarification of the different kinds of constrained devices.
- Every device can be assigned.
- Different characteristics can be assigned.

The categories, characteristics, architectures and device characteristics are simply structured and clearly defined in the model. This can be proven by the overview which can be displayed on one page (see appendix 11.3).

Constrained devices are clearly defined, with the help of limitations. The definition can be found in chapter 6.7.3 and the limitations are listed in chapter 6.9.

The measurements have already shown that all devices can be assigned.

In addition to the category, the individual characteristics can be selected. These characteristics can easily be supplemented by others to remain flexible in case of future developments. At the moment, they are chosen to cover the current standards (see chapter 6.4).

Thus, all requirements were met. Next are the objectives:

- New standards can define which IoT category and which devices are covered.

- An IoT manufacturer can categorize its devices and assign them to the appropriate, existing cybersecurity standards.
- Constrained devices can be identified.
- Defined architectures can be assigned to every device.

The measurements and requirements demonstrate that all objectives have been met. The second objective was modeled as a use case in chapter 7.4 and the different architectures are defined in chapter 6.5 and assigned accordingly to the devices, to the model.

8.3 Proof of Concept

Three application examples prove the feasibility and usefulness of the researched model. The first example is kept simple to illustrate the process, the second example represents a complex case to show that special cases can also be mapped into the model and the third example shows the procedure for a device that is classified as an architecture component.

8.3.1 Example 1

A smart weather station for consumers is used in the first example. The weather station has a touch screen and can be connected to the home network via Wi-Fi. It is no user account necessary to use the device and the weather forecast can be accessed via the Internet.

First, there is the classification in the model: the device is developed for the consumer market, so it is in the category CIoT. Since the device is not used in any critical infrastructure, or does not affect the safety of people, and no private or user-related data is stored, there is no need to add any additional characteristics. Via Wi-Fi over a home router, the connection to the Internet is made. Therefore, architecture 2 is used. The device is a DD, because it is not possible to install third-party software (exclusion criterion for XD) and there are no limitations, which is why it is not a CD. In the case of the characteristics for the device, only number 4 comes into question, since it communicates via IP. The assignment is shown in Table 8.1.

Table 8.1: Example 1: Smart Weather Station

	Category	Characteristic	Architectures	Architecture Component	Device Type	Device Characteristics	Device Limitations
Smart Weather Station	CIoT		2		DD	4	

In the next step, the associated standards and guidelines can be determined. To do this, table 7.1 from chapter 7.1 is filtered according to the criteria from the model. Only the CIoT category and the empty categories are used. Since the device has no other characteristics, all standards with characteristics are dropped. Last, the constraints are filtered. Standards with IP-Communication apply here. Table 8.2 shows all the associated standards.

Table 8.2: Example 1: Guidelines, Standards and Regulations

	Full Name	Category	Characteristics	Restrictions
DIN SPEC 27072 [80]	Informationstechnik - IoT-fähige Geräte - Mindestanforderungen zur Informationssicherheit	CIoT		IP-Communication
EN 62351-3 [120]	Part 3: Communication network and system security - Profiles including TCP/IP	CIoT, EIoT, IIoT		IP-Communication
ENISA Good practices for IoT and Smart Infrastructures Tool [122]	Good practices for IoT and Smart Infrastructures Tool	CIoT, EIoT, IIoT		
ENISA Security and Resilience of Smart Home Environments [124]	Security and Resilience of Smart Home Environments	CIoT		
ETSI EN 303 645 [83]	CYBER; Cyber Security for Consumer Internet of Things	CIoT		
GOV UK - Code of Practice for Consumer IoT Security [97]	Code of Practice for Consumer IoT Security	CIoT		
GSMA IoT Security Guidelines [129]	GSMA IoT Security Guidelines and Assessment	CIoT, EIoT, IIoT		
IoT Security Assurance Framework [131]	IoT Security Assurance Framework	CIoT, EIoT		
ISO/DIS 31700 [132]	[UNDER DEVELOPMENT] Consumer protection — Privacy by design for consumer goods and services	CIoT		
ISO/IEC 20924:2018 [134]	Information technology — Internet of Things (IoT) — Vocabulary	CIoT, EIoT, IIoT		
ISO/IEC 24767-1:2008 [135]	Information technology — Home network security — Part 1: Security requirements	CIoT		
ISO/IEC 30141:2018 [136]	Internet of Things (loT) — Reference Architecture	CIoT, EIoT, IIoT		
ISO/IEC 30147:2021 [137]	Information technology — Internet of things — Methodology for trustworthiness of IoT system/service	CIoT, EIoT, IIoT		
ISO/IEC CD 27403 [139]	[UNDER DEVELOPMENT] Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics	CIoT, EIoT		
ISO/IEC DIS 27400 [140]	[UNDER DEVELOPMENT] Cybersecurity — IoT security and privacy — Guidelines	CIoT, EIoT, IIoT		
NISTIR 8259 [96]	Foundational Cybersecurity Activities for IoT Device Manufacturers	CIoT		
OWASP - IoT Security Guidance [142]	IoT Security Guidance	CIoT, EIoT, IIoT		
SB-327 Information privacy: connected devices [143]	Senate Bill No. 327 CHAPTER 886 TITLE 1.81.26. Security of Connected Devices	CIoT		IP-Communication, Bluetooth-Communication
Secure Design - Best Practice Guide [144]	Secure Design - Best Practice Guide	CIoT, EIoT		

A device manufacturer can quickly and easily obtain a list of the standards and guidelines for his device. Since the device has no limitations (CD and limitations), no exceptions to the standards need to be observed and all provisions apply.

8.3.2 Example 2

The second example is a machine control system for the industrial sector. The machine is located in a company that belongs to the critical infrastructures. For this reason, every employee must log on to the machine control system using a company ID card (with near field communication) before it can be used. Information about the time of logon is stored to trace which employee made changes at what time. The control system has only limited input and output options which relate to the control and monitoring of the machine.

The classification in the model is analogous to the first example, except that there are several properties to consider. The category is IIoT, since it is a device in the industrial sector. The additional characteristics CI, for Critical Infrastructure, SD, because user related data is stored and SY for Safety apply. Which industries belong to the critical infrastructures can be looked up in the laws depending on the country. In Germany, a list can be found over the BSI [112]. In this example, there are more architectures, because the control system can be connected via 5G directly tho the internet or via Wi-Fi to the company network. Therefore, the architectures 1. Direct internet connection (with 5G), 2. Connection over Internet Gateway (company router), 4. Connection over a Gateway (company network segmentation) and 5. Connection over a Switch / Access Point (Wi-Fi Access Point) apply. Since the device is limited in input and output, it is a CD. The limitations are 5. Limited Output and 6. Limited Input. As additional characteristics, the device uses 4. IP-Communication. The assignment is shown in Table 8.3.

Table 8.3: Example 2: Machine Control System

	Category	Characteristic	Architectures	Architecture Component	Device Type	Device Characteristics	Device Limitations
Machine Control System	IIoT	CI,SD,SY	1,2,4,5		CD	4	5,6

Equally to the first example, the associated standards and guidelines are determined by filtering table 7.1 from chapter 7.1. In this case, the IIoT is used. Only standards with the Characteristics PD are dropped, because the Characteristics CI, SD and SY are necessary for this device. For Restrictions, the IP-Communication is used. Table 8.4 shows all the associated standards.

Table 8.4: Example 2: Guidelines, Standards and Regulations

	Full Name	Category	Characteristics	Restrictions
BSI TR-02102-1 [81]	BSI TR-02102-1: ”Cryptographic Mechanisms: Recommendations and Key Lengths” Version: 2021-1	CIoT, EIoT, IIoT	PD, SD, SY	
EN 62351-3 [120]	Part 3: Communication network and system security - Profiles including TCP/IP	CIoT, EIoT, IIoT		IP-Communication
ENISA Baseline Security Recommendations for IoT [121]	Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures	CIoT, EIoT, IIoT	CI	
ENISA Good practices for IoT and Smart Infrastructures Tool [122]	Good practices for IoT and Smart Infrastructures Tool	CIoT, EIoT, IIoT		
ENISA Good Practices for Security of Internet of Things [123]	Good Practices for Security of Internet of Things in the context of Smart Manufactoring	IIoT		
GSMA IoT Security Guidelines [129]	GSMA IoT Security Guidelines and Assessment	CIoT, EIoT, IIoT		
IEC 62443 [130]	Industrial communication networks – Network and system security	IIoT		
ISO/IEC 20924:2018 [134]	Information technology — Internet of Things (IoT) — Vocabulary	CIoT, EIoT, IIoT		
ISO/IEC 30141:2018 [136]	Internet of Things (loT) — Reference Architecture	CIoT, EIoT, IIoT		
ISO/IEC 30147:2021 [137]	Information technology — Internet of things — Methodology for trustworthiness of IoT system/service	CIoT, EIoT, IIoT		
ISO/IEC CD 24392.2 [138]	[UNDER DEVELOPMENT] Information technology — Security techniques —Security reference model for Industrial Internet Platform (IIP)	IIoT		
ISO/IEC DIS 27400 [140]	[UNDER DEVELOPMENT] Cybersecurity — IoT security and privacy — Guidelines	CIoT, EIoT, IIoT		
OWASP - IoT Security Guidance [142]	IoT Security Guidance	CIoT, EIoT, IIoT		

The device in this example is more complex than the first one, but the procedure is the same. The last step and the result are also equivalent and easy to understand. The manufacturer again gets all the necessary standards listed. As the device is constrained (CD), not all provisions from all standards apply. The provisions in the standards can be filtered with the limitations. In this case, 5. Limited Output and 6. Limited Input.

8.3.3 Example 3

The third example is a home router. The device is used to connect a private (home) network to the internet.

For the classification, the category CIoT applies. The device gets the additional characteristics PD and SD, as all data to and from the internet are routed through the device. The router has a direct internet connection and therefore, the architecture 1. As it is an architecture component, it is classified as 1. Internet Gateway. This is also the difference to the previous examples. The device is a DD with no limitations and the characteristics IP-Communication. The assignment is shown in Table 8.5.

Table 8.5: Example 3: Home Router

	Category	Characteristic	Architectures	Architecture Component	Device Type	Device Characteristics	Device Limitations
Home Router	CIoT	PD, SD	1	1	DD	4	

The selection of the standards and guidelines is equally to the first example. But in the restrictions, Gateway and Components 1 is not filtered out. Table 8.6 shows all the associated standards.

Table 8.6: Example 3: Guidelines, Standards and Regulations

	Full Name	Category	Characteristics	Restrictions
BSI TR-02102-1 [81]	BSI TR-02102-1: ”Cryptographic Mechanisms: Recommendations and Key Lengths” Version: 2021-1	CIoT, EIoT, IIoT	PD, SD, SY	
BSI TR-03148 [118]	BSI TR-03148: ”Secure Broadband Router” Version: 2020 1.1	CIoT		Components: 1
DIN SPEC 27072 [80]	Informationstechnik - IoT-fähige Geräte - Mindestanforderungen zur Informationssicherheit	CIoT		IP-Communication
EN 62351-3 [120]	Part 3: Communication network and system security - Profiles including TCP/IP	CIoT, EIoT, IIoT		IP-Communication
ENISA Good practices for IoT and Smart Infrastructures Tool [122]	Good practices for IoT and Smart Infrastructures Tool	CIoT, EIoT, IIoT		
ENISA Security and Resilience of Smart Home Environments [124]	Security and Resilience of Smart Home Environments	CIoT		
ETSI EN 303 645 [83]	CYBER; Cyber Security for Consumer Internet of Things	CIoT		
ETSI TR 103 304 [125]	CYBER; Personally Identifiable Information (PII) Protection in mobile and cloud services	CIoT, EIoT, IIoT	PD	
ETSI TS 103 458 [126]	CYBER; Application of Attribute Based Encryption (ABE) for PII and personal data protection on IoT devices, WLAN, cloud and mobile services - High level requirements	CIoT, EIoT, IIoT	PD	
GOV UK - Code of Practice for Consumer IoT Security [97]	Code of Practice for Consumer IoT Security	CIoT		
GSMA IoT Security Guidelines [129]	GSMA IoT Security Guidelines and Assessment	CIoT, EIoT, IIoT		
IoT Security Assurance Framework [131]	IoT Security Assurance Framework	CIoT, EIoT		
ISO/DIS 31700 [132]	[UNDER DEVELOPMENT] Consumer protection — Privacy by design for consumer goods and services	CIoT		
ISO/IEC 15045-1:2004 [133]	Information technology — Home Electronic System (HES) gateway — Part 1: A residential gateway model for HES	CIoT		Gateway
ISO/IEC 20924:2018 [134]	Information technology — Internet of Things (IoT) — Vocabulary	CIoT, EIoT, IIoT		
ISO/IEC 24767-1:2008 [135]	Information technology — Home network security — Part 1: Security requirements	CIoT		
ISO/IEC 30141:2018 [136]	Internet of Things (loT) — Reference Architecture	CIoT, EIoT, IIoT		
ISO/IEC 30147:2021 [137]	Information technology — Internet of things — Methodology for trustworthiness of IoT system/service	CIoT, EIoT, IIoT		
ISO/IEC CD 27403 [139]	[UNDER DEVELOPMENT] Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics	CIoT, EIoT		
ISO/IEC DIS 27400 [140]	[UNDER DEVELOPMENT] Cybersecurity — IoT security and privacy — Guidelines	CIoT, EIoT, IIoT		
ISO/IEEE 11073-10418:2014 [141]	Health informatics — Personal health device communication — Part 10418: Device specialization — International Normalized Ratio (INR) monitor	CIoT	PD	Personal Health Devices
NISTIR 8259 [96]	Foundational Cybersecurity Activities for IoT Device Manufacturers	CIoT		
OWASP - IoT Security Guidance [142]	IoT Security Guidance	CIoT, EIoT, IIoT		
Regulation (EU) 2016/679 [95]	General Data Protection Regulation	CIoT, EIoT, IIoT	PD	
SB-327 Information privacy: connected devices [143]	Senate Bill No. 327 CHAPTER 886 TITLE 1.81.26. Security of Connected Devices	CIoT		IP-Communication, Bluetooth-Communication
Secure Design - Best Practice Guide [144]	Secure Design - Best Practice Guide	CIoT, EIoT		

8.4 Applications of the Model

The assignment of the model to the devices in the real world has already been described and proven. This chapter is about the application of the model in practice. Six use cases are presented.

8.4.1 Finding Associated Standards

One use case of the model, is the identification of the necessary standards in the development of IoT devices, as already described in Chapter 7.4. In this case, an IoT device manufacturer can map its device in the model and is presented with the associated cybersecurity standards and guidelines through the already existing mapping. It is possible to develop a tool for this purpose, which is not part of this work. The individual requirements of the standards can be transferred into the tool and after the successful assignment of the devices, the tool can output the associated requirements.

This use cast helps device manufacturers produce secure devices because the standards do not have to be searched manually and all important standards and guidelines are displayed even without deep research. No explicit knowledge is required, just the simple software-based mapping process for the researched model.

8.4.2 Security Analysis

The model can also be used as a basis for a security analysis. For this purpose, the categories and characteristics are assigned to a risk. The devices can then be classified in the model and the risks can read off. The whole process can be automated by means of software. An example of this use case is shown in Figure 8.1.

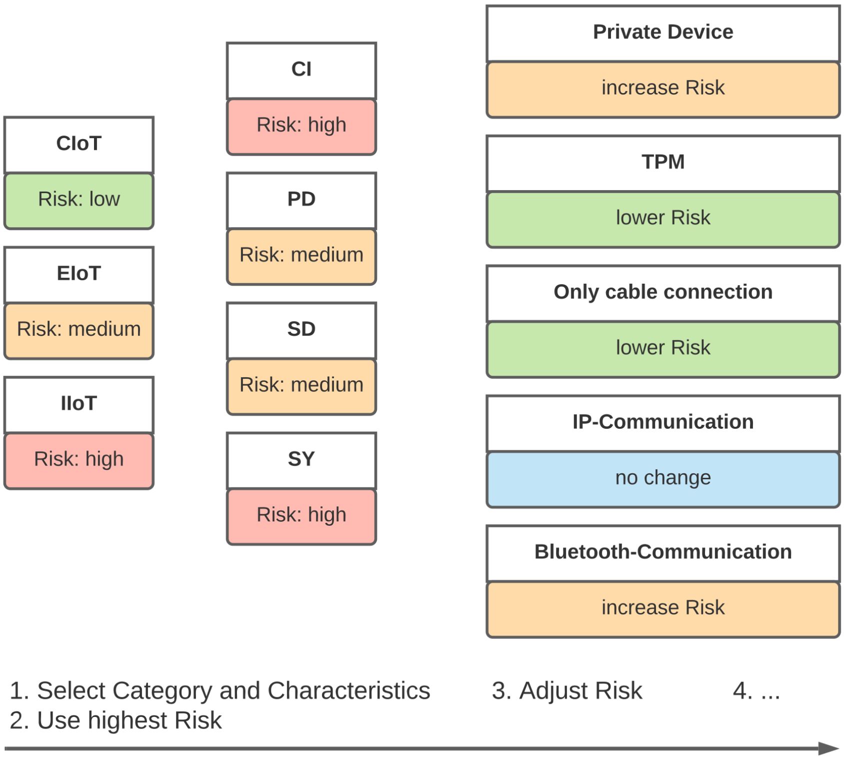


Figure 8.1: Use Case - Security Analysis

In the example in Figure 8.1, the risk of CIoT is low, EIoT medium and IIoT high. The four characteristics CI, PD, SD and SY can change the risk to a higher level. The optional characteristics of the device can change the risk again. For example, a CIoT device starts with a low risk and increases the risk to medium, when sensitive data is processed (SD). If additionally, the device supports a Bluetooth-Communication, the risk can increase further to high.

The procedure is divided into at least three steps, which are also described in Figure 8.1. First, the category and characteristics are determined (Step 1. Select Category and Characteristics), then the highest risk is identified (Step 2. Use highest Risk), and subsequently, depending on further characteristics, the risk is adjusted again (Step 3. Adjust Risk). Additional items can be added as needed, depending on the requirements (optional Step 4. ...). For example, it is possible to define additional characteristics or device properties that change the risk again.

The different risks and steps need to be defined well for every category and the characteristics, but as in every risk analysis, this depends on the concrete application for the risk analysis [146, pp. 26–32]. A precise definition and elaborated procedure of a risk analysis is not part of this thesis.

8.4.3 IoTAG Assistance

Chapter 2.5.1 introduced the IoTAG which will provide a security analysis and a security score based on device data and the current state of the device in the future. The model can be used for an initial assignment and estimation for the score. Similar to the risk analysis, the values of the scoring have to be mapped with the parameters from the model.

8.4.4 Standard Development

Another use case has already been defined as an objective and involves providing assistance to standardization organizations to develop new standards. The restrictions on individual devices and their properties are not the same across all standards at the moment. The model can be used to ensure a uniform definition and assignment.

8.4.5 Tagging

In addition to the standards development, the model is also helpful for scientific publications to clearly define the target group of the research. Current research publications are difficult to categorize (see chapter 4.1) which makes it hard to find relevant research topics. If future publications use the researched model, it ensures an easy classification and a high findability. The best option is to expand the tags with the correct category and optinal add characteristics and architectures, if necessary.

But not only in scientific publications, the model can be used in other areas, too. For example, at conferences to define the scope more precisely or generally, when talking about IoT. Figure 8.2 shows some different possibilities. The inner circle defines the category which should always be specified. The middle circle shows concrete restrictions on devices and the outer circle characteristics which can be added as needed.

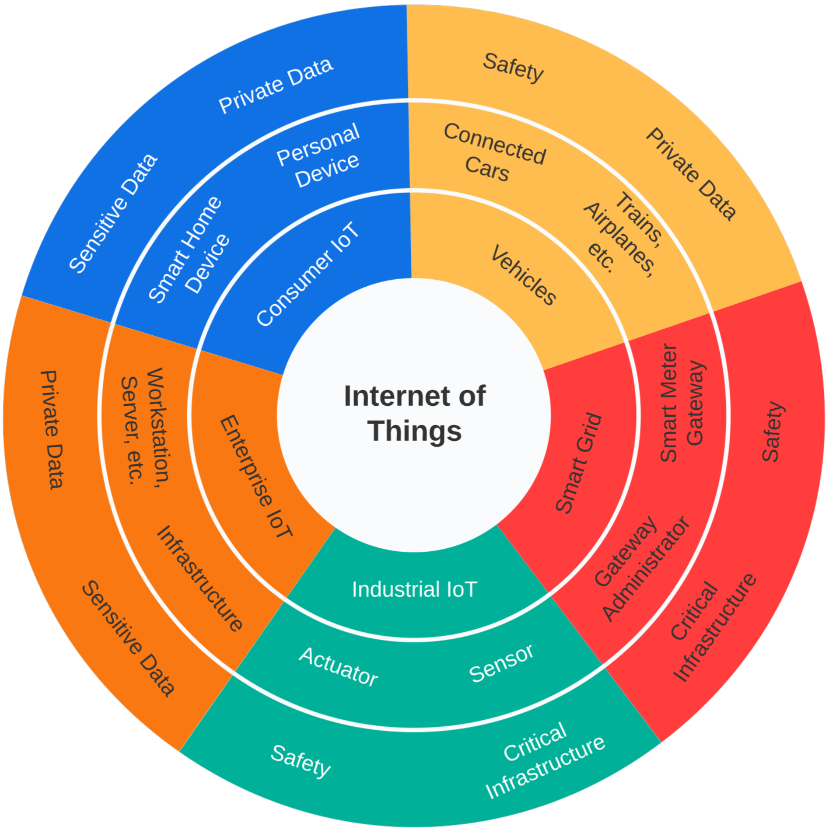


Figure 8.2: Use Case - Tagging

8.4.6 Security- / Privacy- and Usability- Score

The model can be used to research a score for the security, privacy and usability of an IoT device [10]. Depending on the category and the characteristic, the requirements for the three properties are more or less significant.

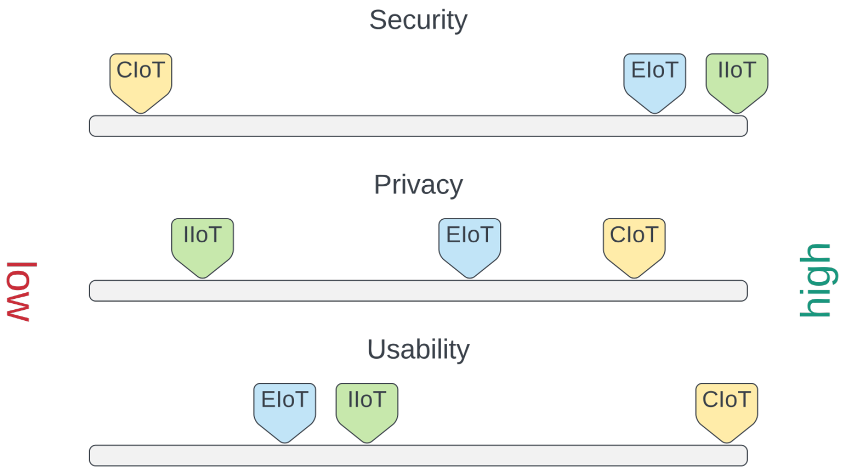


Figure 8.3: Security- / Privacy- and Usability- Score

For example, the scores for Security, Privacy and Usability can be set for each category as shown in Figure 8.3. CIoT gets a low score for Security, while EIoT and IIoT are getting higher values. Depending on additional characteristics, the values change as shown in Figure 8.4, with the additionally characteristic "Private Data". The exact values of the expressions must be researched and precisely defined which is not part of this thesis.

In the example, the requirements for security are low for CIoT (Figure 8.3) and change to a higher value with the characteristic "Private Data" (Figure 8.4), because more security is needed, as private user data is processed. This is also the case for EIoT, but as the value is already very high in the first case, it is only slightly adjusted. The same applies to privacy for all three IoT categories. The requirements for usability are also increasing, as the systems should be easier to use so that the higher safety requirements can also be understood and correctly applied by all users.

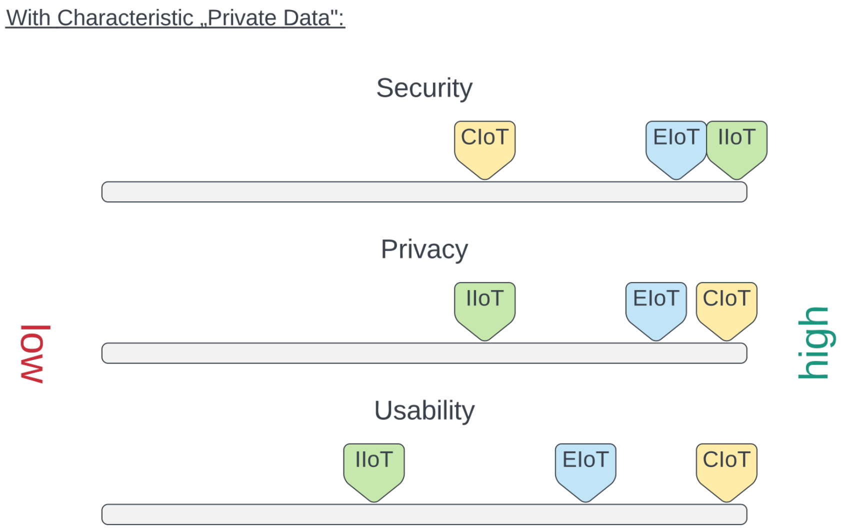


Figure 8.4: Security- / Privacy- and Usability- Score with PD

The scoring system was presented as work in progress at "The Thirteenth International Conference on Cloud Computing, GRIDs, and Virtualization" in Barcelona, Spain in 2022 [10].

8.5 Mapping Tool

In order to be able to map the large number of devices and the rapidly changing standards, a tool will be developed following this thesis that contains all the information and can be expanded dynamically. For this purpose, the standards are stored in a database and linked to the respective categories and characteristics to which they refer. This makes it possible to apply the model by means of software to a new device to be developed, as described in chapter 8.4.1.

Furthermore, the already mapped devices are stored in order to get a current list of already existing devices at any time. This list can be flexibly expanded with new data. By means of extensions and interfaces, the other use cases presented in chapter 8.4 can be integrated into the tool as well.

The process to obtain the standards, is shown graphically in Figure 8.5. The assignment of the device can be implemented as shown in Figure 6.7 in chapter 6.10. The implementation of the tool is not part of the thesis.

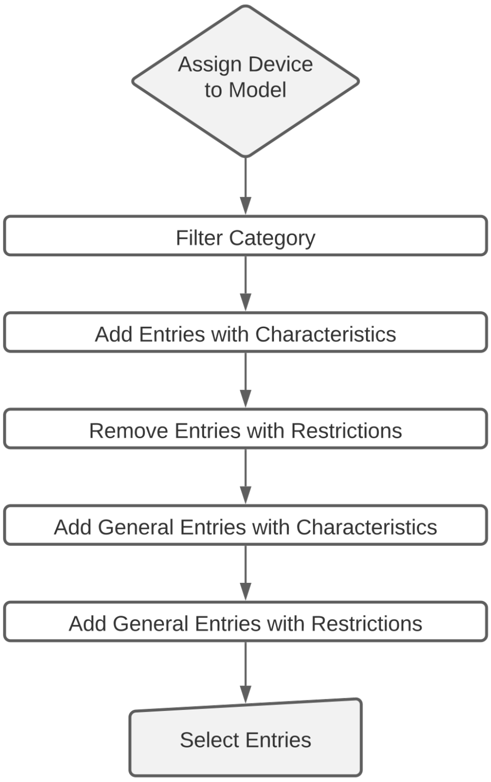

Assign Device to Model
Filter Category
Add Entries with Characteristics
Remove Entries with Restrictions
Add General Entries with Characteristics
Add General Entries with Restrictions
Select Entries

Figure 8.5: Mapping Tool Process

8.6 Further Definitions

As already described in Chapter 5, there are some other categorizations of IoT. These existing solutions are mostly not based on science and not scientifically measurable, according to defined criteria. In comparison, the model in this thesis was researched according to defined objectives (see chapter 6.2). Furthermore, these objectives served to consider the requirements for the model during the research. As a result, the desired use cases can be mapped in the model and even automated. The already existing categorizations can also be transferred to the model, which was shown in Chapter 7.3.

8.7 Feedback on the Model

In previous presentations of the ongoing research, two points were discussed frequently which are briefly explained.

The category or characteristic Health does not exist in the model, because there are no explicit cybersecurity standards for medical devices, yet. If a manufacturer develops devices for medical use, further guidelines must be observed anyway. Including these in the model at this point, would make it more confusing and unnecessarily complex, as it is a special case.

The limitations of a constrained device are not relevant for the assignment to the standards. Nevertheless, they are in the model in order to be able to clearly define a constrained device. If it is clear which device is being developed, the limitations can be excluded and the model simplified.

8.8 Summary

The model fulfills the objectives and provides the desired added value. Since it is flexibly adaptable, it can also be extended for future standards and applications. The use cases show that it has several applications in practice, for example, as an aid for IoT device developers, as a basis for security analyses and as an evaluation for security, privacy and usability. The applications shown, can be automated and implemented as tools, as can the model itself.

Compared to other models and classifications, it was researched independently and scientifically. The goal was to consider the desired use cases already during the research. Therefore, the use cases can be automated and easily implemented.

The model is finished and only needs to be adapted to future developments, if necessary. It can be used without restrictions and is already applicable for the described use cases. Further applications can use the model as a basis and build their research on it.

9 Conclusion

The IoT has many problems regarding cybersecurity. Some of them were presented at the beginning of the thesis, as well as the top 10 vulnerabilities. In addition to the problems, solutions for them were presented, preferably in the form of mandatory standards. Existing policies, or efforts, were further analyzed in terms of their association with IoT devices and their content.

A major problem in the development of standards, and in research in general, is the imprecise and inconsistent definition of IoT and the different sectors. The research question of this thesis was derived from this. Existing efforts in this direction were then analyzed and evaluated in terms of their suitability. However, there was no scientifically based method to make a classification in the case of the IoT. Therefore, a model was researched in this thesis that depicts the IoT world and makes it possible to assign the different aspects of the IoT.

The model is divided into superordinate categories, additional characteristics, architectures, components and devices. The devices are again subdivided and can have both, characteristics and limitations.

To validate the researched model, the devices, standards and existing categories of IoT were assigned and then evaluated. In the process, the model was checked for the objectives and different use cases. All objectives were achieved and the model can be applied in practice.

In the future, the model can be used to quickly find standards to any device and to narrow down the different areas of the IoT. Scientific publications can use the categories to better classify their research.

The model is an up-to-date representation of the IoT world and has been defined accordingly to adapt to the constantly changing conditions. Further research is planned in this regard.

9.1 Further Research

Standardization in the field of IoT has only just begun and current topics such as machine learning or artificial intelligence must be included in future standards and guidelines. While this model is currently valid, it will need to adapt to new technologies in the future. As can be seen from the evaluation, all existing IoT devices can be mapped. Since development is particularly rapid in information technology, the need for an update after a few years cannot be ruled out.

The researched model in this thesis has not yet been applied completely to all existing devices and standards, as this is not possible due to constant new developments and changes. Therefore, in further research on this topic, a tool is under development that supports the mapping and enables a flexible extension of devices and standards as already mentioned in chapter 8.5.

Due to the complexity and different requirements depending on the country, more precise subdivisions for vehicles and smart grid are still missing. These can be expanded in a later version, if required. Likewise, selected areas of the IoT are subject to special requirements, such as medical devices. At the moment, the focus in this area is still on safety, but in the future, cybersecurity will play a greater role and special regulations for medically approved devices cannot be ruled out. If this occurs, the characteristics must be extended.

Depending on future applications, a deeper subdivision of categories or new ones may also become necessary which cannot be covered by the current characteristics. For example, critical infrastructures are increasingly becoming a target for attackers. If there are emerging more stringent guidelines, it may make sense to use a separate category, if other guidelines in the EIoT category are replaced by the new ones.

For the risk analysis use case, research must also be conducted to determine, whether the previous specifications are sufficient or more ones are needed. In the current state, the model is already sufficient for a risk assessment for the IoTAG.

9.2 Summary

In the course of the thesis, the problems of IoT in terms of cybersecurity were identified. For this purpose, security incidents were collected and evaluated, and existing work on the security of IoT was analyzed (e.g., OWASP Top 10 IoT). However, in addition to the identified security issues, there is still the problem of a lack of scientific classification of all IoT areas. For this purpose, a study [2] was created to show the problems in scientific publication. But also in the cooperation with various standards and at conferences, these problems became visible. Therefore, the research and subsequent evaluation of the described model for cybersecurity standards and the categorisation of devices is carried out.

After the model has been fully researched and defined, it can be applied in the IoT world. It serves as a basis for further research on the IoT and cybersecurity and can be used in both, academia and practice.

Scientists and standardization organizations can use it, but also device manufacturers and users. Further research has already been presented and is currently in progress. This includes the mapping tool, the IoTAG, the scoring system and the use in security analyses.

Further development of the model is also desired and research on the model was designed to be correspondingly flexible. Feedback from many sides has already been considered, as several publications on the topic were published during the research period.

10 Bibliography

[1] B. Weber, L. Hinterberger, S. Fischer, and R. Hackenberg, “How to Prevent Misuse of IoTAG?” *CLOUD COMPUTING, The Twelfth International Conference on Cloud Computing, GRIDs, and Virtualization*, pp. 18–23, Apr. 2021.

[2] S. Fischer, K. Neubauer, and R. Hackenberg, “A Study about the Different Categories of IoT in Scientific Publications,” *CLOUD COMPUTING, The Eleventh International Conference on Cloud Computing, GRIDs, and Virtualization*, pp. 24–30, Oct. 2020.

[3] L. Hinterberger, S. Fischer, B. Weber, K. Neubauer, and R. Hackenberg, “IoT Device IdentificAtion and RecoGnition (IoTAG),” *CLOUD COMPUTING, The Eleventh International Conference on Cloud Computing, GRIDs, and Virtualization*, pp. 17–23, Apr. 2020.

[4] L. Hinterberger, S. Fischer, B. Weber, K. Neubauer, and R. Hackenberg, “Extended Definition of the Proposed Open Standard for IoT Device IdentificAtion and RecoGnition (IoTAG),” *International Journal on Advances in Internet Technology*, vol. 13, no. 3 & 4, pp. 110–121, 2020.

[5] K. Neubauer, S. Fischer, and R. Hackenberg, “Security Risk Analysis of the Cloud Infrastructure of Smart Grid and IoT - 4-Level-Trust-Model as a Security Solution,” *International Journal on Advances in Internet Technology*, vol. 13, pp. 11–20, 2020.

[6] J. Graf, K. Neubauer, S. Fischer, and R. Hackenberg, “Architecture of an intelligent Intrusion Detection System for Smart Home,” in *2020 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. Los Alamitos, CA, USA: IEEE Computer Society, Mar. 2020, pp. 1–6.

[7] S. Fischer, K. Neubauer, L. Hinterberger, B. Weber, and R. Hackenberg, “IoTAG: An Open Standard for IoT Device IdentificAtion and RecoGnition,” *SECURWARE 2019, The Thirteenth International Conference on Emerging Security Information, Systems and Technologies*, pp. 107–113, Oct. 2019.

[8] K. Neubauer, S. Fischer, and R. Hackenberg, "Work in Progress: Security Analysis for Safety-critical Systems: Smart Grid and IoT," in *ARCS Workshop 2019; 32nd International Conference on Architecture of Computing Systems*, 2019, pp. 1–6.

[9] K. Neubauer, S. Fischer, and R. Hackenberg, "Risk Analysis of the Cloud Infrastructure of Smart Grid and Internet of Things," *CLOUD COMPUTING, International Conference on Cloud Computing, GRIDs, and Virtualization*, pp. 82–87, May 2019.

[10] S. Fischer, "A Security-, Privacy- and Usability- Scoring System for IoT Devices," *CLOUD COMPUTING, The Thirteenth International Conference on Cloud Computing, GRIDs, and Virtualization*, Apr. 2022.

[11] S. Fischer, "Security-Mindestanforderungen und Standards am Beispiel von OWASP IoT und DIN SPEC 27072." Presented at buildingIoT 2020, Germany, Essen, Mar. 2020.

[12] S. Fischer, "Kategorisierung von IoT Geräten für IT-Sicherheitsstandards." Presented at Gesellschaft für Informatik - Thementag: Sichere Hardware, Germany, Berlin, 2019.

[13] S. Fischer, "IT- Sicherheitsanforderungen im Bereich IoT." Presented at Omnisecure, Germany, Berlin, 2018.

[14] International Electrotechnical Commission(IEC), "ISO/IEC 20924," pp. 1–16, Dec. 2018, accessed on: 24-March-2022. [Online]. Available: https://www.iso.org/standard/69470.html

[15] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The industrial internet of things (IIoT): An analysis framework," *Computers in Industry*, vol. 101, pp. 1–12, 2018.

[16] C. Bai, P. Dallasega, G. Orzes, and J. Sarkis, "Industry 4.0 technologies assessment: A sustainability perspective," *International Journal of Production Economics*, vol. 229, p. 107776, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0925527320301559

[17] European Union Agency for Cybersecurity (ENISA), "Good Practices for Security of Internet of Things," 2018.

[18] Oxford University Press, "enterprise, n." 2021, accessed on: 11-March-2021. [Online]. Available: https://oed.com/view/Entry/62843?rskey=nNkRHO

[19] Oxford University Press, “consumer, n.” 2021, accessed on: 11-March-2021. [Online]. Available: https://www.oed.com/view/Entry/39978

[20] V. S. Gunge and P. S. Yalagi, “Smart Home Automation: A Literature Review,” 2016.

[21] D. Mills, S. Pudney, P. Pevcin, and J. Dvorak, “Evidence-Based Public Policy Decision-Making in Smart Cities: Does Extant Theory Support Achievement of City Sustainability Objectives?” *Sustainability*, vol. 14, no. 1, 2022. [Online]. Available: https://www.mdpi.com/2071-1050/14/1/3

[22] E. Hamilton, “What is Edge Computing: The Network Edge Explained,” 2018, accessed on: 24-March-2022. [Online]. Available: https://www.cloudwards.net/what-is-edge-computing/

[23] Cambridge University Press, “third-party software,” 2022, accessed on: 24-March-2022. [Online]. Available: https://dictionary.cambridge.org/us/dictionary/english/third-party-software

[24] A. Holst, “Number of IoT connected devices worldwide 2019-2030, by vertical,” 2021, accessed on: 26-November-2021. [Online]. Available: https://www.statista.com/statistics/1194682/iot-connected-devices-vertically/

[25] L. S. Vailshery, “Internet of Things (IoT) spending worldwide 2023,” 2021, accessed on: 26-November-2021. [Online]. Available: https://www.statista.com/statistics/668996/worldwide-expenditures-for-the-internet-of-things/

[26] M. Chui, M. Collins, and M. Patel, “IoT value set to accelerate through 2030: Where and how to capture it,” 2021, accessed on: 24-November-2021. [Online]. Available: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/iot-value-set-to-accelerate-through-2030-where-and-how-to-capture-it

[27] M. Chui, M. Collins, and M. Patel, “The Internet of Things: Catching up to an accelerating opportunity,” 2021, accessed on: 5-March-2022. [Online]. Available: https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/iot%20value%20set%20to%20accelerate%20through%202030%20where%20and%20how%20to%20capture%20it/the-internet-of-things-catching-up-to-an-accelerating-opportunity-final.pdf

[28] Bundesamt für Sicherheit in der Informationstechnik (BSI), “Die Lage der IT-Sicherheit in Deutschland 2021,” 2021, accessed on: 5-March-2022. [Online]. Available: https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

[29] Internet Society, “The Trust Opportunity: Exploring Consumer Attitudes to the Internet of Things,” 2019, accessed on: 25-November-2021. [Online]. Available: https://www.internetsociety.org/resources/doc/2019/trust-opportunity-exploring-consumer-attitudes-to-iot/

[30] M. R. Kamdar and M. J. Wu, “PRISM: A Data-Driven Platform for Monitoring Mental Health,” *Pacific Symposium on Biocomputing. Pacific Symposium on Biocomputing*, vol. 21, pp. 33–44, 2016.

[31] S. Gyawali, S. Xu, Y. Qian, and R. Q. Hu, “Challenges and Solutions for Cellular Based V2X Communications,” *IEEE Communications Surveys & Tutorials*, vol. 23, pp. 222–255, 2021.

[32] A. Papathanassiou and A. Khoryaev, “Cellular V2X as the Essential Enabler of Superior Global Connected Transportation Services,” 2017, accessed on: 24-March-2022. [Online]. Available: https://futurenetworks.ieee.org/tech-focus/june-2017/cellular-v2x

[33] 802.11 WG - Wireless LAN Working Group, “IEEE 802.11p-2010,” 2010, accessed on: 24-March-2022. [Online]. Available: https://standards.ieee.org/ieee/802.11p/3953/

[34] Heise Medien GmbH & Co. KG, “Autovernetzung: USA schicken 11p-WLAN in Rente,” 2020, accessed on: 24-March-2022. [Online]. Available: https://www.heise.de/news/Autovernetzung-USA-schicken-11p-WLAN-in-Rente-4966174.html

[35] Die Autobahn GmbH des Bundes, “Intelligente Mobilität für weniger Verkehrsunfälle,” 2021, accessed on: 24-March-2022. [Online]. Available: https://www.autobahn.de/die-autobahn/aktuelles/detail/intelligente-mobilitaet-fuer-weniger-verkehrsunfaelle

[36] Heise Medien GmbH & Co. KG, “Baustellenwarnungen per pWLAN: Auch andere Technik möglich,” 2021, accessed on: 24-March-2022. [Online]. Available: https://www.heise.de/news/Baustellenwarnungen-per-pWLAN-Auch-andere-Technik-moeglich-6034077.html

[37] Bundesamt für Sicherheit in der Informationstechnik (BSI), "Bericht zum Digitalen Verbraucherschutz 2020," 2021, accessed on: 5-March-2022. [Online]. Available: https://www.bsi.bund.de/DE/Service-Navi/Publikationen/DVS-Bericht/dvs-bericht_node.html

[38] H. Gierow, "FOSCAM - IoT-Hersteller ignoriert Sicherheitslücken monatelang," 2017, accessed on: 24-January-2022. [Online]. Available: https://www.golem.de/news/foscam-iot-hersteller-ignoriert-sicherheitsluecken-monatelang-1706-128277.html?utm_source=nl.2017-06-09.html&utm_medium=e-mail&utm_campaign=golem.de-newsletter

[39] O. von Westernhagen, "Hide'n Seek: IoT-Botnetz mit Spionage-Skills," 2018, accessed on: 24-January-2022. [Online]. Available: https://www.heise.de/security/meldung/Hide-n-Seek-IoT-Botnetz-mit-Spionage-Skills-3950938.html

[40] D. Schirrmacher, "OMG-Botnet macht aus IoT-Geräten Proxys," 2018, accessed on: 24-January-2022. [Online]. Available: https://www.heise.de/security/meldung/OMG-Botnet-macht-aus-IoT-Geraeten-Proxys-3982037.html

[41] M. Tremmel, "TORII - Neues IoT-Botnetzwerk ist gekommen, um zu bleiben," 2018, accessed on: 24-January-2022. [Online]. Available: https://www.golem.de/news/torii-neues-iot-botnetzwerk-ist-gekommen-um-zu-bleiben-1809-136860.html?utm_source=nl.2018-10-01.html&utm_medium=e-mail&utm_campaign=golem.de-newsletter

[42] T. Sperlich, "Schweizer Regierungsexperten warnen vor Blackout wegen IoT-Geräten," 2019, accessed on: 24-January-2022. [Online]. Available: https://www.heise.de/newsticker/meldung/Schweizer-Regierungsexperten-warnen-vor-Blackout-wegen-IoT-Geraeten-4413190.html

[43] O. von Westernhagen, "Schwachstellen in P2P-Komponente: Zwei Millionen IoT-Geräte angreifbar," 2019, accessed on: 24-January-2022. [Online]. Available: https://www.heise.de/security/meldung/Schwachstellen-in-P2P-Komponente-Zwei-Millionen-IoT-Geraete-angreifbar-4409298.html

[44] M. Tremmel, "BRICKERBOT 2.0 - Neue Schadsoftware möchte IoT-Geräte zerstören," 2019, accessed on: 24-January-2022. [Online]. Available: https://www.golem.de/news/brickerbot-2-0-neue-schadsoftware-

moechte-iot-geraete-zerstoeren-1906-142153.html?utm_source=nl.2019-06-26.html&utm_medium=e-mail&utm_campaign=golem.de-newsletter

[45] D. Petereit and O. von Westernhagen, “Silex: Neue Malware legt schlecht gesicherte Geräte im Internet of Things still,” 2019, accessed on: 24-January-2022. [Online]. Available: https://www.heise.de/security/meldung/Silex-Neue-Malware-legt-schlecht-gesicherte-Geraete-im-Internet-of-Things-still-4455677.html

[46] J. Schmidt, “Erstmals gezielte Spionage-Angriffe über intelligente Dinge dokumentiert,” 2019, accessed on: 24-January-2022. [Online]. Available: https://www.heise.de/security/meldung/Erstmals-gezielte-Spionage-Angriffe-ueber-intelligente-Dinge-dokumentiert-4489325.html

[47] O. von Westernhagen, “Updates verfügbar: Internetradios von Telestar erlaubten Fernzugriff,” 2019, accessed on: 24-January-2022. [Online]. Available: https://www.heise.de/security/meldung/Updates-verfuegbar-Internetradios-von-Telestar-erlaubten-Fernzugriff-4519870.html

[48] D. Schirrmacher, “Gefährliche Sicherheitslücken in Überwachungskameras von Dahua,” 2019, accessed on: 24-January-2022. [Online]. Available: https://www.heise.de/security/meldung/Gefaehrliche-Sicherheitsluecken-in-Ueberwachungskameras-von-Dahua-4523355.html

[49] M. Tremmel, “DATENLECK - Passwörter zu 515.000 Servern und IoT-Geräten veröffentlicht,” 2020, accessed on: 24-January-2022. [Online]. Available: https://www.golem.de/news/datenleck-passwoerter-zu-515-000-servern-und-iot-geraeten-veroeffentlicht-2001-146146.html?utm_source=nl.2020-01-20.html&utm_medium=e-mail&utm_campaign=golem.de-newsletter

[50] D. Schirrmacher, “Sicherheitsupdates: Angreifer übernehmen Videoüberwachungssysteme von Lilin,” 2020, accessed on: 24-January-2022. [Online]. Available: https://www.heise.de/security/meldung/Sicherheitsupdates-Angreifer-uebernehmen-Videoueberwachungssysteme-von-Lilin-4687883.html?wt_mc=nl.red.ho.ho-nl-daily.2020-03-23.link.link

[51] A. Biselli, “CALLSTRANGER - Große Sicherheitslücke betrifft Millionen UPnP-Geräte,” 2020, accessed on: 24-January-2022. [Online]. Available: https://www.golem.de/news/callstranger-

grosse-sicherheitsluecke-betrifft-millionen-upnp-geraete-2006-148973.html?utm_source=nl.2020-06-09.html&utm_medium=e-mail&utm_campaign=golem.de-newsletter

[52] U. Ries, “Def Con 2020: Millionen von IoT-Geräten im Handumdrehen hackbar,” 2020, accessed on: 24-January-2022. [Online]. Available: https://www.heise.de/news/Def-Con-2020-Millionen-von-IoT-Geraeten-im-Handumdrehen-hackbar-4866178.html?wt_mc=nl.red.ho.ho-nl-daily.2020-08-10.link.link

[53] J. Postel, “DoD standard Internet Protocol,” Internet Requests for Comments, RFC Editor, RFC 760, Jan. 1980.

[54] D. d. Santos, S. Dashevskyi, J. Wetzels, and A. Amri, “AMNESIA:33 How TCP/IP Stacks Breed Critical Vulnerabilities in IoT, OT and IT Devices,” pp. 1–47, Dec. 2020, accessed on: 24-March-2022. [Online]. Available: https://www.forescout.com/resources/amnesia33-how-tcp-ip-stacks-breed-critical-vulnerabilities-in-iot-ot-and-it-devices/

[55] T. Basin, Y. Sade, and Y. Harel, “Research Finds Nearly 70,000 Sensitive Industrial Control Systems Exposed,” 2021, accessed on: 5-Mar-2022. [Online]. Available: https://www.otorio.com/blog/ics-exposures-research-blog/

[56] Open Web Application Security Project (OWASP), “OWASP Internet of Things Project,” 2019, accessed on: 27-May-2021. [Online]. Available: https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project

[57] Open Web Application Security Project (OWASP), “OWASP Internet of Things Top 10,” 2018, accessed on: 27-May-2021. [Online]. Available: https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf

[58] European Union Agency for Cybersecurity (ENISA), “Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures,” Nov. 2017, accessed on: 5-March-2022. [Online]. Available: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

[59] Federal Bureau of Investigation, “Consumer Notice: Internet-Connected Toys Could Present Privacy and Contact Concerns for Children,” 2017, accessed on: 9-Mar-2022. [Online]. Available: https://www.ic3.gov/Media/Y2017/PSA170717

[60] V. Chaudhary, "Semiconductors: Your car is a computer on wheels," 2021, accessed on: 24-November-2021. [Online]. Available: https://www.financialexpress.com/auto/industry/semiconductors-your-car-is-a-computer-on-wheels-maruti-suzuki-cv-raman-electric-cars/2261989/

[61] J. Cronsioe, "A Survey on Security Considerations for Microcontrollers in Traffic Light Networks," 2013, pp. 2–3.

[62] S. Mukherjee, "Smart devices get pandemic boost in U.S. households - Deloitte survey," 2021, accessed on: 24-November-2021. [Online]. Available: https://www.reuters.com/technology/smart-devices-get-pandemic-boost-us-households-deloitte-survey-2021-06-09/

[63] E. Staddon, V. Loscri, and N. Mitton, "Attack Categorisation for IoT Applications in Critical Infrastructures, a Survey," *Applied Sciences*, vol. 11, no. 16, p. 7228, 2021.

[64] C. Thron, K. Tran, D. Smith, and D. S. Benincasa, "Design and simulation of sensor networks for tracking wifi users in outdoor urban environments," in *Defense + Security*, 2017.

[65] T. Alladi, V. Chamola, B. Sikdar, and K.-K. R. Choo, "Consumer IoT: Security Vulnerability Case Studies and Solutions," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 17–25, 2020.

[66] W. Ahmad, A. Rasool, A. R. Javed, T. Baker, and Z. Jalil, "Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey," *Electronics*, 2021.

[67] N. M. Karie, N. M. Sahri, and P. Haskell-Dowland, "IoT Threat Detection Advances, Challenges and Future Directions," *2020 Workshop on Emerging Technologies for Security in IoT (ETSecIoT)*, pp. 22–29, 2020.

[68] B. S. Ahmed, M. Bures, K. Frajták, and T. Cernÿ, "Aspects of Quality in Internet of Things (IoT) Solutions: A Systematic Mapping Study," *IEEE Access*, vol. 7, pp. 13 758–13 780, 2019.

[69] Bundesamt für Sicherheit in der Informationstechnik (BSI), "BSI-TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen," *Technische Richtlinie 02102-1*, p. 22, 2021.

[70] Bundesamt für Sicherheit in der Informationstechnik (BSI), "BSI-TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen," *Technische Richtlinie 02102-2*, p. 8, 2021.

[71] Ren, Kai, “Bluetooth Pairing Part 1 – Pairing Feature Exchange,” 2016, accessed on: 03-June-2021. [Online]. Available: https://www.bluetooth.com/blog/bluetooth-pairing-part-1-pairing-feature-exchange

[72] ANEC, “KEEPING CONSUMERS SECURE - How to tackle cybersecurity threats through EU law,” Nov. 2019, accessed on: 5-March-2022. [Online]. Available: https://www.beuc.eu/publications/beuc-x-2019-066_keeping_consumers_secure_-_how_to_tackle_cybersecurity_threats_through_eu_law.pdf

[73] European Union Agency for Cybersecurity (ENISA), “Security and Resilience of Smart Home Environments,” 2015-12, accessed on: 5-March-2022. [Online]. Available: https://www.enisa.europa.eu/publications/security-resilience-good-practices

[74] G. Lyon, “Nmap: the Network Mapper - Free Security Scanner,” 2022, accessed on: 24-March-2022. [Online]. Available: https://nmap.org

[75] M. Miettinen, S. Marchal, I. Hafeez, N. Asokan, A.-R. Sadeghi, and S. Tarkoma, “Iot sentinel: Automated device-type identification for security enforcement in iot,” in *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS).* IEEE, 2017, pp. 2177–2184.

[76] NortonLifeLock Inc., “How do I purchase Norton Core?” 2021, accessed on: 21-November-2021. [Online]. Available: https://support.norton.com/sp/en/us/norton-core-security/current/solutions/v131932667

[77] Avira Operations GmbH, “Avira SafeThings,” 2021, accessed on: 21-November-2021. [Online]. Available: https://oem.avira.com/en/solutions/safethings-for-router-manufacturers

[78] Avira Operations GmbH, “Avira SafeThings - Securing the Connected Home - Overview White Paper,” 2017, accessed on: 4-December-2020. [Online]. Available: https://safethings.avira.com/res/whitepaper.pdf

[79] L. Nagy and A. Coleşa, “Router-based IoT Security using Raspberry Pi,” in *2019 18th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, 2019, pp. 1–6.

[80] Deutsches Institut für Normung e.V., “Informationstechnik – IoT-fähige Geräte – Mindestanforderungen zur Informationssicherheit,” pp. 1 – 16, 03 2019, accessed on: 3-March-2022. [Online]. Available: https://www.beuth.de/de/technische-regel/din-spec-27072/303463577

[81] Bundesamt für Sicherheit in der Informationstechnik (BSI), “BSI TR-02102-1,” 2021, accessed on: 24-January-2022. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html

[82] Bundesamt für Sicherheit in der Informationstechnik (BSI), “BSI TR-02102-2,” 2022, accessed on: 3-March-2022. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.html

[83] European Telekommunikations Standards Institute (ETSI), “EN 303 645 - Cyber Security for Consumer Internet of Things: Baseline Requirements,” *European Standard*, vol. 2.1.0, 2020.

[84] European Telekommunikations Standards Institute (ETSI), “ETSI TS 103 701,” *European Standard*, Aug. 2021.

[85] The European Parliament and Council, “DIRECTIVE 2014/53/EU,” 2014, accessed on: 4-November-2021. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2014/53/2018-09

[86] European Commission, “Delegierte Verordnung (EU) 2022/30 der Kommission,” Oct. 2021.

[87] Common Criteria Arrangement, “Common Methodology for Information Technology Security Evaluation - Evaluation methodology,” pp. 1–430, May 2017, accessed on: 3-March-2022. [Online]. Available: https://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R5.pdf

[88] International Organization for Standardization (ISO), “ISO/IEC 15408-1,” pp. 1–74, 01 2009, accessed on: 3-March-2022. [Online]. Available: https://www.iso.org/standard/50341.html

[89] Common Criteria Arrangement, “Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model,” pp. 1–106, 05 2017, accessed on: 3-March-2022. [Online]. Available: https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf

[90] Common Criteria Arrangement, “Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components,” pp. 1–323, May 2017, accessed on: 3-March-2022. [Online]. Available: https://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R5.pdf

[91] Common Criteria Arrangement, "Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components," pp. 1–247, May 2017, accessed on: 3-March-2022. [Online]. Available: https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf

[92] The European Parliament and Council, "REGULATION (EU) 2019/881," 2019, accessed on: 24-March-2022. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32019R0881

[93] The European Union Agency for Cybersecurity, "Standardisation and the EU Cybersecurity Act," 2020, accessed on: 8-November-2021. [Online]. Available: https://www.enisa.europa.eu/news/enisa-news/standardisation-and-the-eu-cybersecurity-act-1

[94] European Union Agency for Cybersecurity (ENISA), "Standardisation In Support Of The Cybersecurity Certification," Feb. 2020, accessed on: 5-March-2022. [Online]. Available: https://www.enisa.europa.eu/publications/recommendations-for-european-standardisation-in-relation-to-csa-i

[95] The European Parliament and the Council of the European Union, "REGULATION (EU) 2016/679," *Official Journal of the European Union*, 2016.

[96] M. Fagan, K. Megas, K. Scarfone, and M. Smith, "NISTIR 8259: Foundational Cybersecurity Activities for IoT Device Manufacturers," 2020-5, accessed on: 5-March-2022. [Online]. Available: https://csrc.nist.gov/publications/detail/nistir/8259/final

[97] United Kingdom Department for Digital, Culture, Media & Sport, "Government response to the Regulatory proposals for consumer Internet of Things (IoT) security consultation," 2020, accessed on: 5-March-2022. [Online]. Available: https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security/outcome/government-response-to-the-regulatory-proposals-for-consumer-internet-of-things-iot-security-consultation

[98] Finnish Transport and Communications Agency Traficom, "Finland becomes the first European country to certify safe smart devices – new Cybersecurity label helps consumers buy safer products," 2019, accessed on: 03-June-2021. [Online]. Available:

https://www.kyberturvallisuuskeskus.fi/en/news/finland-becomes-first-european-country-certify-safe-smart-devices-new-cybersecurity-label

[99] International Electrotechnical Commission (IEC), "IEC 62443-4-1," Jan. 2018, accessed on: 5-March-2022. [Online]. Available: https://www.vde-verlag.de/normen/0800517/din-en-iec-62443-4-1-vde-0802-4-1-2018-10.html

[100] K. Greuter, "Evaluating the quality of the international consumer IoT Cyber Security Standard," June 2020, accessed on: 5-March-2022. [Online]. Available: http://essay.utwente.nl/82092/

[101] DIN and DKE, "Deutsche Normungsroadmap IT-Sicherheit," vol. 3, June 2017. [Online]. Available: https://www.dke.de/de/arbeitsfelder/cybersecurity/normungs-roadmap-it-sicherheit

[102] NISTIR, M. Hogan, and B. Piccarreta, "NISTIR 8200: Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT)," pp. 1–185, Nov. 2018.

[103] Google Ireland Limited, "iot - Google Scholar," 2020, accessed on: 8-January-2020. [Online]. Available: https://scholar.google.de/scholar?start=0&q=iot

[104] Google Ireland Limited, "internet of things - Google Scholar," 2020, accessed on: 8-January-2020. [Online]. Available: https://scholar.google.de/scholar?start=0&q=internet+of+things

[105] A. Selamat and Z. Iqal, "Open Challenges in Internet of Things Security," *Journal of Physics: Conference Series*, vol. 1447, p. 012054, Jan. 2020.

[106] J. Gubbi, R. Buyya, S. Marusic, and M. S. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *ArXiv*, vol. abs/1207.0203, 2013.

[107] M. Gleißner, J. Dotzler, J. Hartig, A. Aßmuth, C. Bulitta, and S. Hamm, "IT Security of Cloud Services and IoT Devices in Healthcare," in *CLOUD COMPUTING 2021 : The Twelfth International Conference on Cloud Computing, GRIDs, and Virtualization.*

[108] H. Zuerner, "The Internet of Things as greenfield model: A categorization attempt for labeling smart devices," *2014 IEEE World Forum on Internet of Things (WF-IoT)*, pp. 5–9, 2014.

[109] J. E. Ibarra-Esquer, F. F. Gonzälez-Navarro, J. S. Sänchez, B. L. Flores-Rïos, M. A. Astorga-Vargas, and M. L. Gonzälez-Ramïrez, "Graphical Framework for Categorizing Data Capabilities and Properties of Objects in the Internet of Things," *IEEE Access*, vol. 8, pp. 22 366–22 377, 2020.

[110] E. Siow, T. Tiropanis, and W. Hall, "Analytics for the Internet of Things," *ACM Computing Surveys (CSUR)*, vol. 51, pp. 1–36, 2018.

[111] Beecham Research, "World of IoT Sector Map," 2021, accessed on: 24-March-2022. [Online]. Available: https://www.beechamresearch.com/download-details/world-of-iot-sector-map/

[112] BSI and BBK, "Kritische Infrastrukturen - Definition und Übersicht," 2020, accessed on: 5-Mar-2022. [Online]. Available: https://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/einfuehrung_node.html

[113] Bundesminister des Innern, "Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement," 2011, accessed on: 4-May-2022. [Online]. Available: https://www.bbk.bund.de/SharedDocs/Downloads/DE/Mediathek/Publikationen/KRITIS/bmi-schutz-kritis-risiko-und-krisenmanagement.pdf?__blob=publicationFile&v=9

[114] D. Stylianos, "Towards privacy definition for hybrid sensitivity data," 2017.

[115] International Organization for Standardization (ISO), "ISO/IEC 27000:2018 - Information technology — Security techniques — Information security management systems — Overview and vocabulary," Feb. 2018.

[116] International Electrotechnical Commission(IEC), "IEC 62304:2006 - Medical device software — Software life cycle processes," May 2006, accessed on: 02-May-2022. [Online]. Available: https://www.iso.org/standard/38421.html

[117] Bundesamt für Sicherheit in der Informationstechnik (BSI), "BSI TR-03148: Secure Broadband Router," Apr. 2020, accessed on: 5-March-2022. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03148/TR03148.pdf;jsessionid=6EC4D7E4317F5F4696843C98109CF01B.internet472?__blob=publicationFile&v=1

[118] Bundesamt für Sicherheit in der Informationstechnik (BSI), "BSI TR-03148: Secure Broadband Router," 2020, accessed on: 9-May-2022.

[Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03148/TR03148.pdf;jsessionid=BC1F9C47CF466E71F8CC4F3A8CA59368.internet472?__blob=publicationFile&v=1

[119] DIN Deutsches Institut für Normung e. V., "DIN EN 60335-1:2020-08," 2020, accessed on: 24-January-2022. [Online]. Available: https://www.beuth.de/en/standard/din-en-60335-1/324269153

[120] DIN Deutsches Institut für Normung e. V., "DIN EN 62351-3 VDE 0112-351-3:2019-06," 2019, accessed on: 24-January-2022. [Online]. Available: https://www.vde-verlag.de/standards/0100528/din-en-62351-3-vde-0112-351-3-2019-06.html

[121] European Union Agency for Cybersecurity (ENISA), "Baseline Security Recommendations for IoT," 2017, accessed on: 24-January-2022. [Online]. Available: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

[122] European Union Agency for Cybersecurity (ENISA), "Good practices for IoT and Smart Infrastructures Tool," 2019, accessed on: 24-January-2022. [Online]. Available: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool

[123] European Union Agency for Cybersecurity (ENISA), "Good Practices for Security of Internet of Things," 2018, accessed on: 24-January-2022. [Online]. Available: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot/at_download/fullReport

[124] European Union Agency for Cybersecurity (ENISA), "Security and Resilience of Smart Home Environments," 2015, accessed on: 24-January-2022. [Online]. Available: https://www.enisa.europa.eu/publications/security-resilience-good-practices

[125] European Telekommunikations Standards Institute (ETSI), "CYBER; Personally Identifiable Information (PII) Protection in mobile and cloud services," 2016, accessed on: 24-January-2022. [Online]. Available: https://www.etsi.org/deliver/etsi_tr/103300_103399/103304/01.01.01_60/tr_103304v010101p.pdf

[126] European Telekommunikations Standards Institute (ETSI), "CYBER; Application of Attribute Based Encryption (ABE) for PII and personal

data protection on IoT devices, WLAN, cloud and mobile services - High level requirements," 2018, accessed on: 24-January-2022. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/103400_103499/103458/01.01.01_60/ts_103458v010101p.pdf

[127] UN Task Force on Cyber Security and Over-the-Air issues, "Draft Recommendation on Cyber Security of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 GRVA," 2018, accessed on: 24-January-2022. [Online]. Available: https://unece.org/fileadmin/DAM/trans/doc/2018/wp29grva/GRVA-01-17.pdf

[128] UN Task Force on Cyber Security and Over-the-Air issues, "Draft Recommendation on Software Updates of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 GRVA," 2018, accessed on: 24-January-2022. [Online]. Available: https://unece.org/fileadmin/DAM/trans/doc/2018/wp29grva/GRVA-01-18.pdf

[129] GSM Association, "GSMA IoT Security Guidelines and Assessment," 2020, accessed on: 24-January-2022. [Online]. Available: https://www.gsma.com/iot/iot-security/iot-security-guidelines/

[130] International Electrotechnical Commission (IEC), "Industrial communication networks – Network and system security," 2021, accessed on: 24-January-2022. [Online]. Available: https://www.iec.ch/blog/understanding-iec-62443

[131] IoT Security Foundation, "IoT Security Assurance Framework," 2021, accessed on: 24-January-2022. [Online]. Available: https://www.iotsecurityfoundation.org/wp-content/uploads/2021/11/IoTSF-IoT-Security-Assurance-Framework-Release-3.0-Nov-2021-1.pdf

[132] International Organization for Standardization (ISO), "ISO/DIS 31700," 2004, accessed on: 24-January-2022]. [Online]. Available: https://www.iso.org/standard/76772.html

[133] International Organization for Standardization (ISO), "ISO/IEC 15045-1:2004," 2018, accessed on: 24-January-2022. [Online]. Available: https://www.iso.org/standard/26313.html

[134] International Organization for Standardization (ISO), "ISO/IEC 20924:2018," 2018, accessed on: 24-January-2022. [Online]. Available: https://www.iso.org/standard/69470.html

[135] International Organization for Standardization (ISO), “ISO/IEC 24767-1:2008,” 2008, accessed on: 24-January-2022. [Online]. Available: https://www.iso.org/standard/43880.html

[136] International Organization for Standardization (ISO), “ISO/IEC 30141:2018,” 2021, accessed on: 24-January-2022. [Online]. Available: https://www.iso.org/standard/65695.html

[137] International Organization for Standardization (ISO), “ISO/IEC 30147:2021,” 2021, accessed on: 24-January-2022. [Online]. Available: https://www.iso.org/standard/53267.html

[138] International Organization for Standardization (ISO), “ISO/IEC CD 24392.2,” 2022, accessed on: 24-January-2022. [Online]. Available: https://www.iso.org/standard/78703.html

[139] International Organization for Standardization (ISO), “ISO/IEC CD 27403,” 2022, accessed on: 24-January-2022. [Online]. Available: https://www.iso.org/standard/78702.html

[140] International Organization for Standardization (ISO), “ISO/IEC DIS 27400,” 2022, accessed on: 24-January-2022. [Online]. Available: https://www.iso.org/standard/44373.html

[141] International Organization for Standardization (ISO), “ISO/IEEE 11073-10418:2014,” 2014, accessed on: 24-January-2022. [Online]. Available: https://www.iso.org/standard/61897.html

[142] Open Web Application Security Project (OWASP), “IoT Security Guidance,” 2018, accessed on: 24-January-2022. [Online]. Available: https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=Main

[143] Senate of California, “Senate Bill No. 327 CHAPTER 886,” 2018, accessed on: 24-January-2022. [Online]. Available: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327

[144] IoT Security Foundation, “Secure Design - Best Practice Guide,” 2019, accessed on: 24-January-2022. [Online]. Available: https://www.iotsecurityfoundation.org/wp-content/uploads/2019/12/Best-Practice-Guides-Release-2_Digitalv3.pdf

[145] Trusted Computing Group, “TCG TPM 2.0 Automotive Thin Profile For TPM Family 2.0; Level 0,” 2018, accessed on: 24-January-2022.

[Online]. Available: https://trustedcomputinggroup.org/resource/tcg-tpm-2-0-library-profile-for-automotive-thin/

[146] Bundesamt für Sicherheit in der Informationstechnik (BSI), "BSI-Standard 200-3: Risk Analysis based on IT-Grundschutz," 2018, accessed on: 5-May-2022. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2003_en_pdf.pdf

11 Appendix

11.1 Big Picture - IoT Network

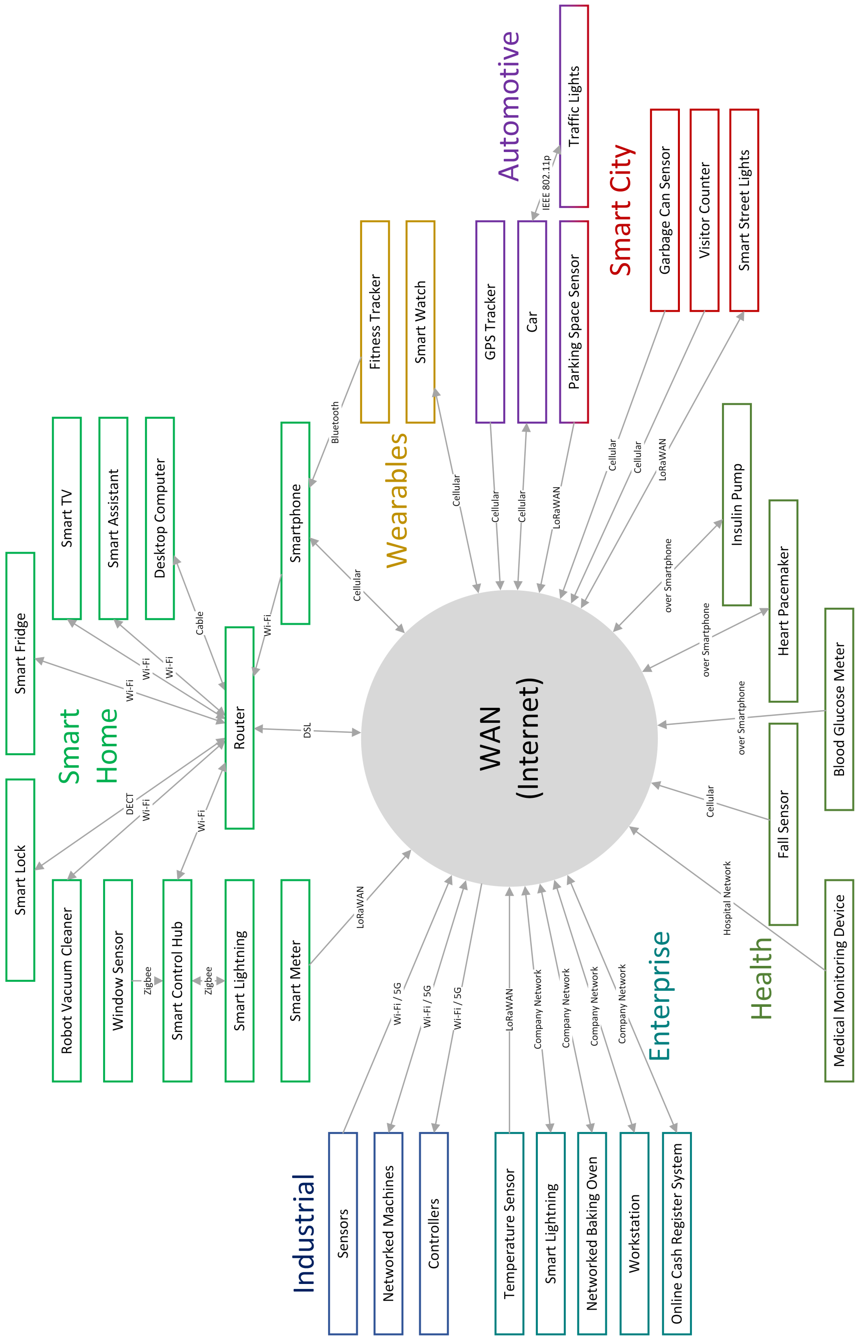


Figure 11.1: Big Picture - IoT Network

11.2 Architecture of Categories

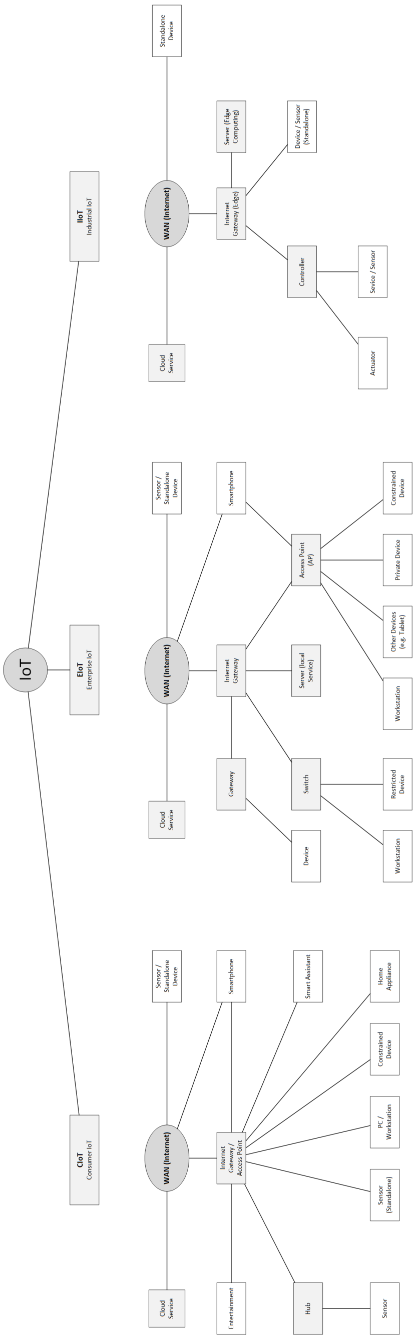
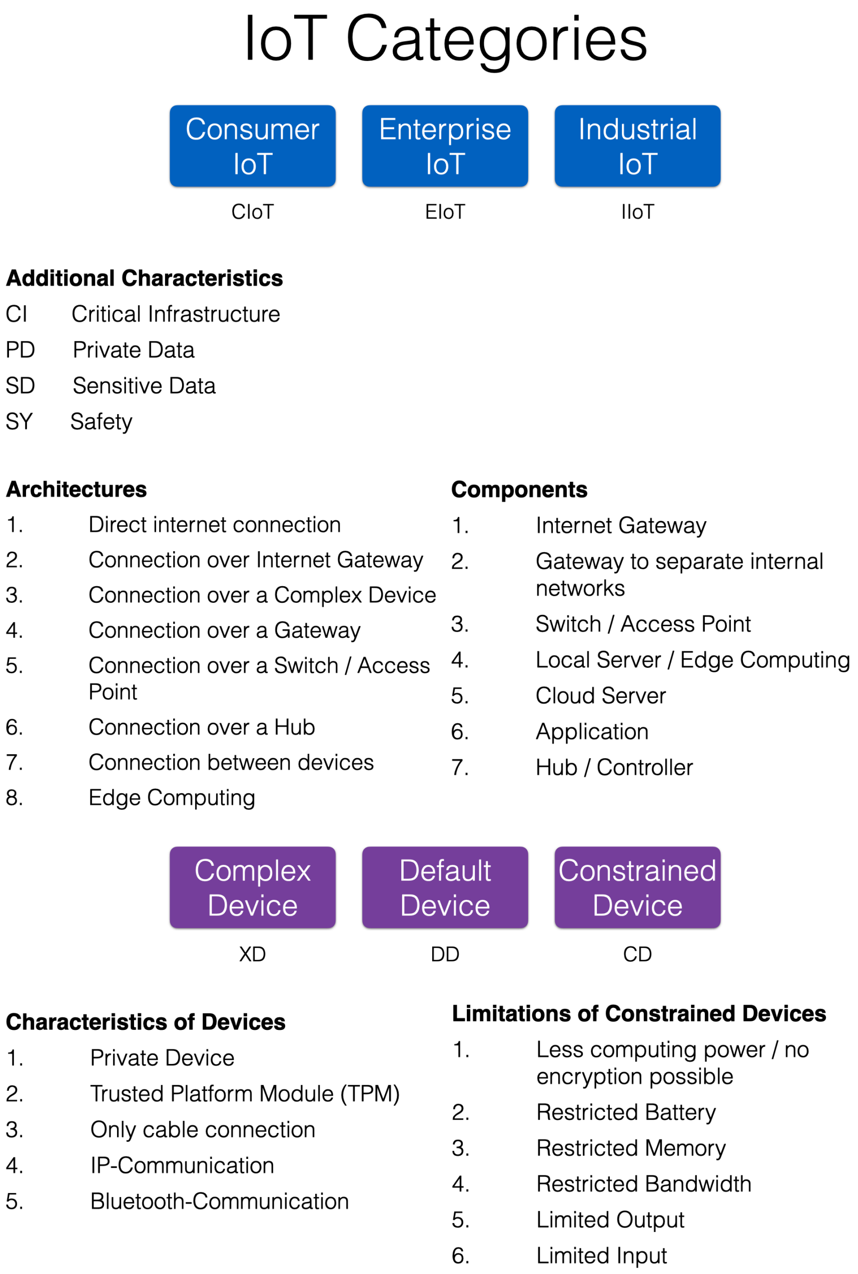


Figure 11.2: Architecture of Categories

11.3 Overview of the Categorization



IoT Categories

Additional Characteristics

CI	Critical Infrastructure
PD	Private Data
SD	Sensitive Data
SY	Safety

Architectures

1. Direct internet connection
2. Connection over Internet Gateway
3. Connection over a Complex Device
4. Connection over a Gateway
5. Connection over a Switch / Access Point
6. Connection over a Hub
7. Connection between devices
8. Edge Computing

Components

1. Internet Gateway
2. Gateway to separate internal networks
3. Switch / Access Point
4. Local Server / Edge Computing
5. Cloud Server
6. Application
7. Hub / Controller

Characteristics of Devices

1. Private Device
2. Trusted Platform Module (TPM)
3. Only cable connection
4. IP-Communication
5. Bluetooth-Communication

Limitations of Constrained Devices

1. Less computing power / no encryption possible
2. Restricted Battery
3. Restricted Memory
4. Restricted Bandwidth
5. Limited Output
6. Limited Input

Figure 11.3: Overview of the Categorization

11.4 Mapping: IoT Devices - Categorization

Table 11.1: Categorization of IoT Devices

		Category	Characteristic	Architectures	Component	Device Type	Device Characteristics	Device Limitations
Ambient Assistant Living	**Camera**	CIoT	S,PD	2		DD	4	
Ambient Assistant Living	**Person Fall Detection Sensor (Bluetooth)**	CIoT	S	6		CD	5	1,2,3,4,5,6
Ambient Assistant Living	**Person Fall Detection Sensor (Wi-Fi)**	CIoT	S	2		CD	4	2,3
Business	**Airport Display**	EIoT		2		CD	(3),(4)	3
Business	**Car Charging Station**	EIoT		2,6		DD	4	
Business	**Online Cash Register System**	EIoT	SD	2		DD	2,(3),4	
Business	**Paket Tags RFID**	EIoT		6		CD		1,2,3,4,5,6
Business	**Price Tags (e.g., 6LOWPAN)**	EIoT		6		CD	4	1,2,3,4,5,6
Business	**Private Smartphone**	EIoT	PD	1,2		XD	1,2,4	
Business	**Server Sensor (e.g., Temperatur)**	EIoT		2		CD	4	1,2,3,4,5,6
Business	**Signage (Wi-Fi)**	EIoT		2		CD	4	3
Business	**Vending machine with 3G**	EIoT		1		DD	4	
Connected Car	**Connected Car**	EIoT	CI,PD,SY	1		DD	1,4,5	
Connected Car	**LighEIoT Control**	EIoT	CI,SY	1		CD	4	3
Connected Car	**Toll Station**	EIoT		1		CD	4	3
Health	**Bluetooth Health Sensor**	CIoT	PD, SY	6		CD	5	1,2,3,4,5,6
Health	**Connected Equipment in Hospitals**	EIoT	PD, SY	4		DD		
Health	**Medical Connected Device at Doctor**	EIoT	PD,SY	4		DD	(3),(4)	
Health	**Medical ImplanEIoT**	CIoT	PD,SY	3,6		CD	5	1,2,3,4,5,6
Health	**Medical Operation Equipment**	EIoT	SY	4		DD		
Health	**Wireless Health Sensor (e.g., Zigbee)**	CIoT	PD, SY	6		CD		1,2,3,4,5,6
Health	**Blood Pump**	CIoT	PD,SY	4		DD		
Industrial	**3G Factory Sensor / Controller**	IIoT	(SD),(SY)	1		DD	4	
Industrial	**6LOWPAN Sensor**	IIoT		1		CD	4	2,3,4,5,6
Industrial	**Bluetooth Factory Sensor / Controller**	IIoT	(SD),(SY)	4		CD	5	(1,2,3,4,5,6)
Industrial	**Device in Critical Infrastructure (e.g., for Water or Nuklear plant)**	IIoT	CI,(SD),(SY)	4		DD	3	
Industrial	**LighEIoTensor**	IIoT		4,6		CD		1,2,3,4,5,6
Industrial	**Other Remote Factory Sensor / Controller**	IIoT	(SD),(SY)	4,6		CD		1,2,3,4,5,6

		Category	Characteristic	Architectures	Component	Device Type	Device Characteristics	Device Limitations
Industrial	**Packaging**	IIoT		4,6		CD		1,2,3,4,5,6
Industrial	**Piplines in Factory**	IIoT		4,6		CD		1,2,3,4,5,6
Industrial	**Pump Control**	IIoT	(SD),(SY)	4,6		CD		1,2,3,4,5,6
Industrial	**Smart Farming Device**	IIoT		1		DD	4	
Industrial	**Wi-Fi Factory Sensor / Controller**	IIoT	(SD),(SY)	4		DD	4	
Industrial	**Wind Turbine**	IIoT	CI,(SD),(SY)	1		DD	4	
Network	**Network Storage**	All	(PD),(SD)	2		XD	3,4	
Network	**Router**	All	(PD),(SD)		1			
Network	**Server**	EIoT	(PD),SD	2		XD	2,3,4	
Network	**Switch**	All	(PD),(SD)		3			
Office	**Heating Actuator (Wi-Fi)**	EIoT		2		DD	4	
Office	**Heating Control System**	EIoT		2		DD	4	
Office	**Lightsensor (e.g., Zigbee)**	EIoT		2,6,7		CD		1,2,3,4,5,6
Office	**Security Cam**	EIoT	PD,SD	2		DD	4	
Office	**Smoke Detector (Bluetooth)**	EIoT	SY	2,6		CD	5	1,2,3,4,5,6
Personal	**Child Toy with Camera**	CIoT	PD,SD	2		CD	4	3,4
Personal	**Child Tracker**	CIoT	SD	1		CD	4	2,3,4
Personal	**Laptop**	CIoT	PD,SD	2		XD	2,4,5	
Personal	**Laptop with 3G**	CIoT	PD,SD	1,2		XD	2,4,5	
Personal	**Smartphone**	CIoT	PD,SD	1,2		XD	2,4,5	
Private	**3G GPS Tracker for Private Cars**	CIoT	SD	1		DD	4	
Private	**3G ODB Dongle**	CIoT	SD	1		DD	5	
Private	**Battery (Solar Storage)**	CIoT / SG		2		DD	4	
Private	**Digital Camera**	CIoT	PD,SD	2		DD	4	
Private	**Drone**	CIoT	PD,SD,SY	3		DD		
Private	**eBook Reader**	CIoT		2		DD	4,5	
Private	**Game Console**	CIoT	PD	2		XD	4	
Private	**Headset**	CIoT		3		CD	5	1,2,3,4,5
Safety	**Connected Devices in Emergency Cars (e.g., Ambulance)**	EIoT	CI,SY	1		DD		
Smart Home	**3G Smart Home Device**	CIoT	(PD),(SD)	1		DD	4	
Smart Home	**3G Temperature Sensor**	CIoT		1		DD	4	
Smart Home	**Bluetooth Smart Home Device**	CIoT	(PD),(SD)	2,3,6		CD	5	1,2,3,4,5,6
Smart Home	**Bluetooth Temperatur Sensor**	CIoT		2,3,6		CD	5	2,3,4,5
Smart Home	**BT Door Lock**	CIoT		3		CD	5	2,3
Smart Home	**Charging Station**	CIoT		2,6		DD	4	
Smart Home	**Garage Door Opener (Wi-Fi)**	CIoT		2		DD	4	
Smart Home	**Google Assistant**	CIoT	PD,SD	2		DD	4,5	
Smart Home	**Lightbulb**	CIoT		2,6,7		CD		1,2,3,5
Smart Home	**Other Wireless Smart Home Device (e.g., Zigbee)**	CIoT	(PD),(SD)	2,6		CD		1,2,3,4,5,6
Smart Home	**Receiver with Speaker**	CIoT		2		DD	4,5	
Smart Home	**Security Cam**	CIoT	PD,SD	2		DD	4	
Smart Home	**Smart Home Hub**	CIoT	PD,SD		7			
Smart Home	**Smart TV**	CIoT	PD,(SD)	2		XD,DD	4,5	

		Category	Characteristic	Architectures	Component	Device Type	Device Characteristics	Device Limitations
Smart Home	**Smoke Detector**	CIoT	SY	2		DD	4	
Smart Home	**Washer / Dryer**	CIoT		2		DD	4	
Smart Home	**Webcam**	CIoT	PD,SD	2		DD	4	
Smart Home	**Wi-Fi Temperature Sensor**	CIoT		2		DD	4	
Smart Home	**WiFi Door Lock**	CIoT		2,3		DD	4	
Smart Meter	**Smart Meter**	EIoT	CI,PD,SD	6		CD	3	1,2,3
Smart Meter	**Smart Meter Gateway**	EIoT	CI,PD,SD		1			
Transportation	**3G GPS Tracker for Trucks**	EIoT	CI,PD,SY	1		DD	4	
Transportation	**Aircraft**	EIoT	CI,SY					
Transportation	**Airport Terminal**	EIoT	CI,SY	4		DD	4	
Transportation	**Rail Sensor**	EIoT	CI,SY					
Transportation	**Ship**	EIoT	CI,SY					
Wearable	**Wearable 3G (Smart Watch)**	CIoT	PD	1,2,3		DD	4,5	
Wearable	**Wearable Bluetooth (Fitness Tracker)**	CIoT	PD	3		CD	5	4
Wearable	**Wearable Wi-Fi (Smart Watch)**	CIoT	PD	2,3		DD	4,5	

11.5 Curriculum Vitae

Mein Lebenslauf wird aus Gründen des Datenschutzes in der elektronischen Fassung meiner Arbeit nicht veröffentlicht.

11.6 Zusammenfassung

Die Vernetzung von physischen Geräten, einschließlich ihrer Infrastruktur und Daten, wird als Internet of Things bezeichnet. Die Zahl der vernetzten Geräte hat in den letzten Jahren stetig zugenommen und wird auch in Zukunft weiter steigen. Dies führt ebenfalls zu einer steigenden Zahl von Angriffen auf diese Geräte, welche als potenziell unsicher eingestuft sind. Die Gründe für die mangelnde IT-Sicherheit sind vielfältig und führen zum Beispiel zu Botnetzen und ähnlichen Problemen.

Verbindliche Normen und Richtlinien können dazu beitragen, die IT- Sicherheit zu gewährleisten, auch wenn die Entwicklung der Geräte schnell und kostengünstig ablaufen soll. In einigen Bereichen ist die Entwicklung solcher Richtlinien bereits weit fortgeschritten, idealerweise länderübergreifend als europäischer Standard. Probleme bei der Normung sind jedoch die unterschiedlichen Definitionen von Gerätekategorien und damit die Zuordnung eines Gerätes zu einer Norm.

Selbst in der Wissenschaft sind die Definitionen und Kategorien für Geräte des Internet of Things nicht eindeutig oder fehlen ganz. Das macht es schwierig, relevante Publikationen zu finden. Daher wurde ein Internet of Things Modell erforscht, um diese Probleme zu lösen und klare Kategorien zu definieren.

Das Modell unterteilt die Welt des Internet of Things in Kategorien, ergänzt die Definitionen mit Merkmalen und unterscheidet die verschiedenen Gerätetypen. Auch die Architekturen und zugehörigen Komponenten werden berücksichtigt. Das Modell kann auf alle Geräte und verfügbaren IT-Sicherheitsstandards angewandt werden, was durch deren Abbildung auf das Modell gezeigt wird. Die Anwendungen in der realen Welt sind vielfältig und werden als verschiedene Use Cases dargestellt. Da sich die Digitalisierung schnell weiterentwickelt, ist das erforschte Modell so konzipiert, dass es sich flexibel an neue Entwicklungen anpassen lässt.