IoT Security With INFINITE: The 3-Dimensional Internet Of Things Maturity Model

Christoph Haar[1] Erik Buchmann[2]

Abstract:

Many companies are more and more interested in using IoT devices, either to optimize their processes or due to the lack of alternatives. The situation is similar to some years ago, when cameras were banned on company premises for security considerations, but all modern cell phones had cameras. Observations have shown, that the security properties of IoT devices with a similar functionality might differ significantly. This makes it challenging for a company to identify IoT devices that match its security policy. In order to make it possible for companies to assess the level of security of IoT devices before buying them, we introduce INFINITE, our 3-dimensional INternet oF thINgs maturITy modEl. INFINITE can be used at procurement-time, to find out to which degree an IoT device meets the requirements of the company's security policy. This simplifies the procurement process, prevents the introduction of IoT devices that cannot be integrated into an enterprise-wide security strategy, and ultimately saves costs. To this end, INFINITE allows us to considers both the software and the hardware life cycle of an IoT device.

1 Introduction

Today, many companies are using IoT devices to optimize their processes [SKG19]. For example, in agriculture IoT devices are used to measure soil properties, such as moisture, and forward the data [El18]. With this information, the optimal time to water the soil can be determined. Many different kinds of IoT devices from an incalculable number of manufacturers exist, which are subject to different legal security requirements [HR20; Lo19]. Thus, security properties of the IoT devices vary greatly. This makes it difficult for companies to find out, which device can be integrated into a company-wide security strategy. This is a major problem, because insecure devices can be an attractive target for attackers. For example, company data can fall into the wrong hands [Po16] or IoT devices can end up as part of a botnet [Ko17]. For this reason, companies must evaluate whether an IoT device provides certain security practices before acquisition. Those security practices must be provided across the entire life cycle of the IoT device.

[1] Hochschule für Telekommunikation, Datenschutz und Sicherheit in Informationssystemen, Gustav-Freytag-Str. 43-45, 04277 Leipzig, Deutschland haar@hft-leipzig.de

[2] Hochschule für Telekommunikation, Datenschutz und Sicherheit in Informationssystemen, Gustav-Freytag-Str. 43-45, 04277 Leipzig, Deutschland buchmann@hft-leipzig.de

Maturity models are a prominent way to evaluate the security of IT processes or IT systems [CAW10; LH17]. Typically, maturity models evaluate two dimensions: (a) whether a certain security practice is considered and (b) which maturity level a security practice has reached. To the best of our knowledge, there is no maturity model that allows to evaluate the security of IoT devices, and does so over the entire period of use. To do this, a maturity model must be expanded to include the device's life cycle as a third dimension.

In this paper, we introduce INFINITE, the 3-dimensional INternet oF thINgs MaturITy modEl. With INFINITE the security of IoT devices will be measurable and assessable. In this way, different IoT devices can be compared with each other according to three objective dimensions. The X-Axis represents „IoT Security Practices", that are used to secure IoT devices. The Y-Axis represents „IoT Maturity Level", that every security practice can reach. Finally, the Z-Axis represents the „IoT Life Cycle", which considers whether a security practice is available over the life cycle of a device.

To define the three axes, we derive security practices for IoT devices from the IT Grundschutz Compendium Module „SYS.4.4 General IoT Devices", developed by the German Federal Office for Information Security (BSI) [Fe19]. We identify the cycle phases of IoT devices by a literature review. Finally, we compare maturity models in IT security to define maturity levels suitable for INFINITE. To evaluate our maturity model, we introduce a scenario in which a company plans to procure three different IoT devices. Fur this purpose, we evaluate the security of a total of 60 IoT devices with INFINITE in a case study and compare the results.

Paper structure: Section 2 reviews related work. In Section 3, we develop the three axis of INFINITE. The evaluation of INFINITE with a case study follows in section 4. Section 5 concludes.

2 Related Work

In this section, we review related work according to life cycles, security practices and maturity level.

2.1 IoT Life Cycle Approaches

Internet of Things (IoT) means adding sensors or communication interfaces to conventional devices such as refrigerators or TVs, to provide additional functions. Thus, not only the hardware-life cycle of the IoT device, but also a software-life cycle must be considered. The life cycle of a conventional device ends as soon as its hardware is physically worn out. With IoT devices, every device also has a software-life cycle. This life cycle ends, as soon as the service time ends, or the manufacturer does no longer provide security updates [BH20]. Thus, an IoT device must be out of service due to security considerations, even it is physically in mint condition.

Many IoT life cycle approaches exist in literature, that introduce different phases for the software and the hardware life cycle of IoT devices. The authors vary the number and designation of the life cycle phases. For example, Rahman defined five different life cycle phases for hardware and software of an IoT device [ROL18]. Soós defined 8 life cycle phases [So18], Yousefnezhad [YMF20] and Selimis [Se20] only three. However, the life cycle phases have a similar content. A life cycle begins with the planning and construction of the IoT device. During this phase, the software of the IoT device is developed and the hardware is produced. This is followed by installation and commissioning. The IoT device is physically connected to the power outlet and the software is connected to the network. In the next phase, the IoT device is operated and the service used. Some of the authors mentioned, also

add security updates to this phase. At the end of the life cycle follows the retirement or decommission of the IoT device.

2.2 IoT Security Basics

IoT security is no longer a marginal issue. There are numerous official guidelines for IoT security. For example the German Federal Office for Information Security (BSI) defined several threats and security practices for IoT devices in the IT Grundschutz Compendium Module „SYS.4.4 General IoT Devices“ [Fe19]. Another official guideline was published by the National Institute of Standards and Technology (NIST) in December 2020 [Na20]. This guideline includes a total of four draft documents concerning IoT core baseline and non-technical supporting capability for manufacturers and federal government. The International Organization for Standardization (ISO) published the „ISO/IEC 27400 - Cybersecurity - IoT security and privacy - Guidelines“ as a draft in 2021. This draft includes guidelines on risks, principles and controls for security and privacy of IoT. The central aim of these official guidelines is to ensure that the security of companies that are using IoT devices can be audited. In addition to these guidelines, numerous other publications address IoT security practices. For example, Microsoft [Mi21] and Kaspersky [Ka21] published best practices for IoT security on their websites.

However, these guidelines and best practices do not consider threats and security practices for the hardware of IoT devices. If an IoT device is used outdoors, it is exposed to the elements or vandalism. Therefore, it must be protected from water and dust [LE20] or willful destruction [Ah17; Cl21] too. Furthermore, the IoT device must be protected from hardware exploitation [Al20] in which an attacker could use unprotected communication interfaces like open USB ports for an attack.

2.3 Defining Maturity Level

Maturity models for IT security are often used in companies to get information about the performance of a security practice. The information provided by the maturity models help the companies to find out which security practices should be improved. There are many institutions that defined their own maturity models for different use cases in IT security. The Computer Emergency Response Team (CERT) for example developed the resilience management model [CAW10] for improving the resilience of business processes. Pamela Curtis developed the cyber security capability model [CMS15] to protect critical infrastructure from cyber threats. Another security metrics framework called IBM security framework [In13a] was developed by International Business Machines (IBM). This framework serves as a security gap analysis between business and technology. The International Organization of Standardization (ISO) developed the information security management system [In13b] which improves the security of information systems through security standards. The National Institute of Standards and Technology (NIST) developed the Security Metrics Guide for Information Technology Systems [Sw17]. Table 1 summarizes the maturity level of each institution.

All maturity level, we are aware of have common grounds. First of all, the individual maturity level always build on each other. So there is a clear gradation from the lowest to the highest maturity level. The lowest maturity level means that a security practice is not implemented at all. The highest maturity level represents an advanced implementation of a security practice that cannot be improved any more, according to all knowledge available. Another common aspect is, that reaching a certain maturity level means, that all levels below it are also fulfilled. For example, a maturity level three means that the requirements from all level below are also implemented. We refer to this procedure, when defining the maturity level for INFINITE in the next section.

Tab. 1: Security Maturity Models

Maturity Level	CERT	Curtis	IBM	ISO	NIST
1	Incomplete	Not Performed	Initial	Performed	Evolving
2	Performed	Initiated	Basic	Managed	Def. and Doc.
3	Managed	Performed	Capable	Established	Well Establ.
4	Defined	Managed	Efficiency	Predictable	Self-Regen.
5	-	-	Optimizing	Optimized	-

3 Defining INFINITE

In this section, we define the IoT Life Cycle, IoT Security Practices and IoT Maturity Level for INFINITE. based on the literature review from Section 2. We start with the definition of the IoT life cycle by checking which of the life cycle phases mentioned in Section 2 are required for INFINITE from a corporate customers view. After that, we define the IoT Security Practices by generalizing the security practices described in the official guidelines. Finally, we define the IoT Maturity Level based on the introduced pattern from Section 2.

3.1 IoT Life Cycle

Our objective is to support the security evaluation of IoT devices at purchase-time. Thus, we leave aside the planning, design and the construction phase of an IoT device. We focus on risks that arise after the company has purchased an IoT device. From a life cycle point of view, the first risk that must be considered is that the device was already insecure or tampered with at the time of purchase. The last risk might arise from a sorted out but still functional IoT device that can contain sensitive data. It must be possible to replace outdated security practices by security updates for example. In addition, it must be ensured that it is not possible for an attacker to get access or gain unencrypted data after switching on the IoT device. To prevent such risks, INFINITE allows to consider all life cycle phases from the procurement to the decommission. In order to prevent this risk, INFINITE must be able to check whether security practices have already been implemented at the time of purchase. After the IoT device has been delivered to the company, it must be installed in the next step. To do this, the IoT device is connected to a power outlet and the network. In this phase, INFINITE must also check whether all security practices are available e.g. to prevent the network's login information will be disclosed. After the IoT device was commissioned successfully, the operation phase starts. Of course, INFINITE must be able to check, whether all security practices are available over the entire use of the IoT device. After the operation phase, the last phase of the life cycle of an IoT device begins. The device is permanently disconnected from the power outlet and the network and will be disposed. Since sensitive data could still be stored on the IoT device after disposal, it is important that INFINITE checks whether the security practices are still available after the disposal of the IoT device. Thus, we consider four life cycle phases for INFINITE, as defined in Table 2.

3.2 IoT Security Practices

In section 2, we introduced several official guidelines and best practices for IoT security. However, these guidelines and best practices not only include the security of IoT devices, but also consider

Tab. 2: INFINITE Life Cycle Phases

Life Cycle Phase	Definition
Procurement	This phase represents the first phase of the life cycle and describes the period between the purchase and the handover of the IoT device to the company.
Commission	This phase describes the physical connection of the IoT device to the power outlet and the connection to the companies network.
Operation	This phase starts after the IoT device has been successfully commissioned and lasts over the entire period of use.
Decommission	This phase represents the final phase of the life cycle. It starts as soon as the IoT device has been disconnected permanently from the power outlet and the network.

methods for a secure use like restriction of network access [Fe19]. Because the aim of INFINITE is to evaluate the security of IoT devices, we only consider security practices from the official guidelines that affect the security of the IoT device itself. Another aim of INFINITE is to evaluate the security of a wide variety of IoT devices. To achieve this aim, the security practices must be formulated as widely as possible.

Since we want INFINITE to assess how well an IoT device matches the requirements of the company's security strategy, we restrict the scope of the security practices to the IoT device itself. That is, we leave aside, say, how well an operator is trained to use the device, or if a backup strategy for IoT devices exist. We base the set of practices to be considered on IT Grundschutz Compendium Module „SYS.4.4 General IoT Devices“ [Fe19].

One security practice mentioned is authentication. With authentication INFINITE allows to check, whether the IoT device is using any method that helps to establish trust between IoT device and the server or user. Another important security practice of an IoT device mentioned in SYS.4.4 General IoT Devices is encryption. That includes encrypted communication to ensure confidential data exchange between the IoT device and the server or user. It also means encrypted data storage. We assume that every IoT device does at least store WLAN credentials that needs to be encrypted. Furthermore, we exclude cloud storage. In this case, the data will not be stored on the IoT device itself. Therefore, INFINITE allows to check, whether the IoT device is using any method that ensures encrypted communication and encrypted data storage on the IoT device.

A third security practice of IoT devices mentioned in SYS.4.4 General IoT Devices are security updates. A security update is maintaining or improving the security of an IoT device. Due to this fact, with INFINITE it can be checked, whether the IoT device is provided with security updates by the manufacturer. There are different types of updates, such as function updates, which ensure that an IoT device receives new functions. In case the new function maintains or improves the security of the IoT device, we consider this function to be a security update. All other updates that do not address the security of an IoT device are not considered by INFINITE. Because IoT devices can be exposes to the elements, we also consider water and dust protection. That means INFINITE allows to check, whether the IoT device is using any method to protect the hardware from ingress of water and dust.

We do not consider extreme events like natural hazards, fire, attacks or vandalism because such events will destroy the most IoT devices. Table 3 summarizes all security practices for INFINITE.

Tab. 3: INFINITE Security Practices

Security Practices	Definition
Authentication	Authentication is including any method that enables trust between the IoT device and the server or user.
Encrypted Communication	Encrypted Communication is including any method that ensures confidential data exchange between the IoT device and the server or user.
Encrypted Data Storage	Encrypted Data Storage is including any method that ensures confidential data storage on the IoT device.
Security Updates	Security Updates will be provided by the manufacturer and maintain or improve the security of an IoT device.
Water and Dust Protection	Water and Dust Protection is including any method that prevents physical damage from water and dust ingress.

3.3 IoT Maturity Level

The maturity level should indicate, how well a security practice has been implemented. The lowest maturity level is not implementing a security practice at all. The next better level of maturity is to provide some kind of support to circumvent security issues, without actually implementing a suitable measure. It is challenging to distinguish meaningful maturity level for practices that have been implemented. Assume one IoT device guarantees encrypted communication with AES, and a second one uses RC4. Both IoT devices are using encrypted communication, but RC4 is considered insecure by now. Thus, the latter device should have a lower maturity level for the security practice „encrypted communication“. However, it is not feasible to integrate any encryption approach in INFINITE.

To approach this issue, we borrow from the well-described states of technology [IT20]: The lowest state of technology is called „generally accepted rules of technology“. This means that a certain implementation of a security practice is widely in use, has a low degree of innovation, and its use should be part of the general education of any developer of an IoT device. In contrast, a security practice is „state of the art“, if it is the best solution for a security goal that is currently available on the market. On top of that, „existing scientific knowledge and research“ refers to newly researched security practices, which have a prototypical implementation (if any). Because INFINITE only considers IoT devices that have left the prototype status, we do not need to consider this state of technology. In the best case, a manufacturer of an IoT device implements a state of the art security practice, and has the implementation or implementation process certified by an auditor.

After we checked, to which state of technology a certain security practice can corresponds to, we now use the pattern from Section 2 to define the IoT Maturity Level for INFINITE. The worst possible performance will occur, if the manufacturer does not even perform the security practice at all. This condition will represent the lowest maturity level. The second maturity level will be reached, if a certain security practice is not performed but at least some other kind of measures are provided by the manufacturer. The third maturity level will be reached, when the manufacturer does at least perform the security practice corresponding to generally accepted rules of technology. If the manufacturer does perform the security practice corresponding to state of the art, the fourth maturity level will be reached. The best case will occur, if a manufacturer performs a state of the art security practice certified by an auditor. In this case, the fifth and highest maturity level that represents the best possible performance will be reached.

From these specifications, we define the following maturity level for INFINITE as shown in Table 4.

Tab. 4: INFINITE Maturity Level

Maturity Level	Definition
Not Performed	This level represents the lowest maturity level. The manufacturer does *not perform* the security practice at all or does not give any information about it.
Initial	The manufacturer does still not perform the security practice but alternatively offers *initial* measures.
Performed	The manufacturer does *perform* the security practice corresponding to generally accepted rules of technology.
Improved	The manufacturer *improved* the performance of the security practice corresponding to state of the art.
Optimized	This level represents the highest maturity level. The manufacturer does perform the security practice corresponding to state of the art and *optimized* it in form of a certification by an auditor.

3.4 IoT Device Properties

Before using INFINITE, it is necessary to identify needed product properties of the IoT devices. For example, if one IoT device only has an IP54 rating and another one provided the more secure IP68, INFINITE evaluate both equally. This is because both IP54 and IP68 are certified and state of the art security practices. In case that an IoT device is needed, that could be submerged underwater, an IP54 rating would not be sufficient although both devices were rated equally. For this purpose INFINITE can be used to check whether or not a security practice is performed and state of the art, but not to identify which state of the art security practices is more secure.

4 Evaluation

In this section, we evaluate INFINITE by using a case study approach.

In particular, we use INFINITE to evaluate the security properties of three different IoT device classes. For each IoT device class, we evaluate the security of a total of 20 IoT devices. After that, we analyze our findings.

4.1 Conception

With our evaluation, we want to find out, which applications are conceivable for INFINITE. Generally, INFINITE is used to evaluate the security of IoT devices. On the one hand, the security of IoT devices with a similar application scenario could be evaluated. Therefore, it is important to find out, if INFINITE is able to meaningfully distinguish IoT devices with a similar application scenario. On the other hand, the security IoT devices with completely different application scenarios could be evaluated. That means, it is also interesting to find out, if INFINITE is able to meaningfully distinguish IoT devices with a different application scenario. Furthermore, we implemented the life cycle as a third dimension to INFINITE. That means, INFINITE also considers the life cycle of an IoT device

when evaluation its security. This raises the question of whether INFINITE can identify changes in the maturity level of a certain security practice over the entire life cycle of an IoT device. In order to evaluate the security of an IoT device with INFINITE, it is also necessary to obtain the needed information in a first place. That means, information about the availability of security practices of an IoT device must be obtained. Due to this fact the question arise, if all information needed by INFINITE can be obtained by a simple web search and without a direct contact to the manufacturer. After the evaluation has been implemented, the management must decide which IoT devices can be procured. This decision is based on the company's security policy. Thus, it is also important to find out, if INFINITE is able to identify IoT devices that comply with an organization's security policy. To be able to make such a decision, it is also interesting to identify differences between the implementation of security practices for the IoT devices over the life cycle. Thus, we analyze the evaluation results of INFINITE to identify different implementations of security practices over the life cycle.

For this purpose, we will answer the following questions:

- Is it possible to use INFINITE to evaluate the security of IoT devices with different application scenarios?
- Is it possible to use INFINITE to evaluate the security of IoT devices with similar application scenarios?
- Can INFINITE identify changes in the maturity level of a security practice over the life cycle?
- Can all information needed by INFINITE obtained without contacting the manufacturer?
- Can INFINITE be used to identify IoT devices that comply with an organization's security policy?
- Is it possible to use INFINITE's evaluation results to reveal different implementations of security practices over the life cycle?

Scenario *A drug manufacturer plans to use several IoT devices. To increase the security, it is planned to procure a smart* ***IoT smoke detector*** *that is able to send an alarm to the user's smartphone in case of smoke detection. Furthermore, a smart* ***IoT security camera*** *to monitor company premises and sending livestreams to the user's smartphone should also be procured. Finally, it is also planned to procure a smart* ***IoT temperature sensors*** *to log the cooling chain of the stored drugs. Because its IT infrastructure is mission critical, the drug manufacturer has a security policy. This policy states that only equipment may be used on company premises, that complies with state of the art with regard to its security properties.*

IoT Devices Based on our scenario, we define three IoT device categories. For each category, we choose 20 IoT devices. In this way, we evaluate the security of a total of 60 IoT devices. Only IoT devices that can be controlled with a smartphone via WLAN connection are considered. In addition, the manufacturer must advertise the IoT device on its own website. In this way, information about the security of an IoT device can be obtained directly from the manufacturer.

Table 5 illustrates the IoT device categories and all 60 IoT devices that fulfill the mentioned requirements for our evaluation.

Procedure To obtain all information required for INFINITE's evaluation, we define the following procedure. The **first step** is to search the manufacturers website, where the IoT device is presented

Tab. 5: IoT Devices

IoT Security Cameras	IoT Temperature Sensors	IoT Smoke Detectors
Vandal WDR [Ha21]	Aqara Temp. Sensor [Lu21a]	Gigaset [Gi21]
EufyCam 2C [An22b]	SONOFF SNZB-02 [SO21]	Banggood [Ba21]
Tapo C310 V1 [TP22]	ELV HmIP-WTH-2 [EL21a]	LH-601WF [Ch21]
Google Nest [Go21]	RSH Temp. Sensor [Tu22]	PA-443W [SZ20]
5MP PTZ [Re21]	Nous E6 [No22]	HS1SA [Sh16]
Laxihub O1 [Ar20]	Temp. Reader [Ha22b]	Wi-Fi Smoke Detector [Do22]
Arlo Ultra [Ar21]	Long Range Sensor [Na21]	Frient Smoke Alarm [Fr22a]
IPC-HDBW5831E [Da21]	Shelly H&T [Al22]	ABUS Detector [AB22]
D-Link H.265 [Re21]	Zemismart Sensor [Ze22a]	HmIP-SWSD [EL21b]
Axis P1447 [EX21]	Tesla Sensor [TE22]	Bosch Smoke Alarm [Ro22b]
WV-X8570N [iP21]	Wireless Sensor [Di22]	Anka Smoke Alarm [An22a]
Cam IR [Va21]	Govee Hygrometer [Go22]	SH8-99101UK [Sm22]
IP Tube [iP21]	Frient Sensor [Fr22b]	R7049 [Ki22]
LUPUS-LE281 [Lu21b]	Bosch Thermostat [Ro22a]	Photoel. Detector [Ha22a]
H.264 960P [Kk16]	Temperature Logger [Sh20]	DWL-2600AP [DL20]
IP9165-HP [VI16]	Climate Sensor [Ne20a]	Nedis Detector [Ne20b]
DS-2CD2025FWD-I [Hi16]	Smart Home 400 [Dy20]	Zemismart Sensor [Ze22b]
IPC-B650H-Z [In16]	Proteus AMBIO [Pr21]	Fibaro Sensor [FI22]
Cisco Video [Ci13]	Multi.Sensor [Ae21]	ELRO Connects [Co20]
Smart Outdoor Cam [Ne16]	Bresser Hygrometer [Br21]	PSG01 [Ph21]

or offered. In this way, all security information provided by the manufacturer can be viewed and documented. These information can be product descriptions or a frequently asked question (FAQ) sections directly on the website. Also downloadable documents like data sheet with technical specifications or user manuals might be provided on the website. In case there is still information needed to evaluate the security of the IoT device, the **second step** is to search websites of vendors who also sell the IoT device. It is common for vendors to provide information about the IoT device to be selled. If there is still information needed, the **third step** is a web search for third-party information about the IoT device. If available, technical reviews or security reports provide detailed, in-depth information about an IoT device from an independent party. Such reports might also include information the manufacturer does not necessarily want to disclose. In case, there is still not all information obtained, we have to assume, the security practice is not implemented for the IoT device.

We apply this procedure to all 60 IoT devices.

Evaluation Framework and Assumptions In order to make INFINITE's evaluation results comparable, it is necessary to define a consistent evaluation basis for all IoT devices. For this purpose, we define an evaluation framework. In this evaluation framework, we determine which conditions an IoT device has to met for each security practice, in order to reach a certain maturity level.

Table 6 illustrates the evaluation framework for each security practice and maturity level, considered by INFINITE.

Tab. 6: Evaluation Framework

Security Practice	Maturity Level
Authentication	**not performed:** The security practice is not available or there is no information. **initial: performed:** We consider SSL as performed because it is a commonly used authentication protocol but the successor protocol TLS is already available. **improved:** We consider TLS as improved because it is the latest authentication protocol and commonly used Extensible Authentication Protocol (EAP) is used in WPA2. WPA3 was already released as the successor to WPA2 but not all devices can implement the WPA3 standard. Thus, EAP is state of the art. Also AES in CCM ensures data authentication. We consider it improved, because there is currently no successor algorithm and it is commonly used. **optimized:** The use of TLS is certified by an official auditor.
Encrypted Communication and encrypted data storage	**not performed:** The security practice is not available or there is no information. **initial:** The manufacturer offers alternative measures like access restrictions to protect the data. **performed:** We consider DES or blowfish encryption as performed because it is still in use but tripple DES or AES with 128 bit are more secure. **improved:** Symmetric AES encryption with at least 128 bit, tripple DES and asymmetric RSA encryption is improved because there is currently no successor algorithm and it is commonly used. **optimized:** The use of AES with at least 128 bit or tripple DES is certified by an official auditor
Security Updates	**not performed:** The security practice is not available or there is no information. **initial:** The manufacturer offers alternative measures like customer support. **performed:** Security updates has to be installed manually by the user. **improved:** Automatic security updates make it possible to distribute new firmware quickly without the user having to search for it. **optimized:** If automatic security updates are certified by an official auditor, we consider authentication as optimized.
Water and Dust Protection	**not performed:** The security practice is not available or there is no information. **initial:** The manufacturer offers the purchase of additional hardware that protects the IoT device. **performed:** The manufacturer states that the hardware is protected from dust and water ingress. **improved:** The manufacturer provides more detailed information about the degree of protection. **optimized:** The protection from water and dust ingress is certified by an official auditor Like the IP Rating.

Furthermore, we make some assumptions for our evaluation, illustrated in Table 7. With these assumptions, we specify the evaluation framework by defining rules that are not covered by the evaluation framework.

Tab. 7: Assumptions

Adress	Assumption
Security Practices	In case there is no information about a certain security practice, we consider the security practice as not performed for security reasons. Furthermore, we consider a security practice to be performed in case there is information available that the security practice is implemented but no detailed information whether the security practice is certified or state of the art.
Security Updates	Regular security updates are important for the device security. If the last security update was more than one year ago, we consider the security practice as not performed.
Availability	If an IoT device is using authentication protocols like TLS or encryption algorithms like AES, we assume that these protocols and algorithms are available for the entire life cycle. Same holds any security practices that protect the IoT device from water and dust ingress.

4.2 Case Study

In this section, we apply the evaluation procedure for the first IoT security camera as an example.

4 MP Vandal WDR Fixed Dome Network Camera The manufacturer states on the website that the 4 MP Vandal WDR Fixed Dome Network Camera [Ha21] uses TLS certificates for *authentication*. We assume that TLS will be used over the entire life cycle. Since TLS is the successor to SSL and currently state of the art, we consider authentication as *improved* for every life cycle phase. The manufacturer also states on the website that the 4 MP Vandal WDR Fixed Dome Network Camera uses *encrypted communication* via HTTPS. Because HTTPS is used with TLS, we consider the security practice *encrypted communication* as *improved* for every life cycle phase. The manufacturer also provides a specification section for the 4 MP Vandal WDR Fixed Dome Network Camera on the website. This section states, that for example passwords are protected. In this case, at least the WLAN credentials are encrypted. The manufacturer also offers a manual guide for the 4 MP Vandal WDR Fixed Dome Network Camera on the website. In this guide, the option to use an encrypted memory card is described. The data on the memory card remains encrypted after the user chose this option. That means, it is generally possible to store encrypted data over the entire life cycle. However, it stays unclear how the data will be encrypted. It is conceivable that a state of the art encryption algorithm like AES is used but it is not guaranteed. Due to this fact, we consider the security practice *encrypted data storage* as *performed* for every life cycle phase. In the manual guide it is also recommended to install the latest firmware update. The latest firmware is available on the website. The description about firmware updates in the user manual states that updates has to be installed manually. Thus, we have to assume that automatic updates are not available. Automatic security updates would be state of the art. Manually installed security updates require a regular search for new security updates by the user. This is not state of the art. Furthermore it is unclear if security updates are available after reaching the decommission phase. Thus, we consider the security practice *security updates* as *performed* for every life cycle phase except the decommission phase. The manufacturer also provides information about the physical protection of the 4 MP Vandal WDR Fixed Dome Network Camera. It is protected against water and dust ingress corresponding to IP67 [DS21]. Since IP67 refers to a certified level of protection and does not degrade over time, we consider the security practice *water and dust protection* for every life cycle phase as *optimized*.

Figure 1 illustrates the evaluation results of the 4 MP Vandal WDR Fixed Dome Network Camera.

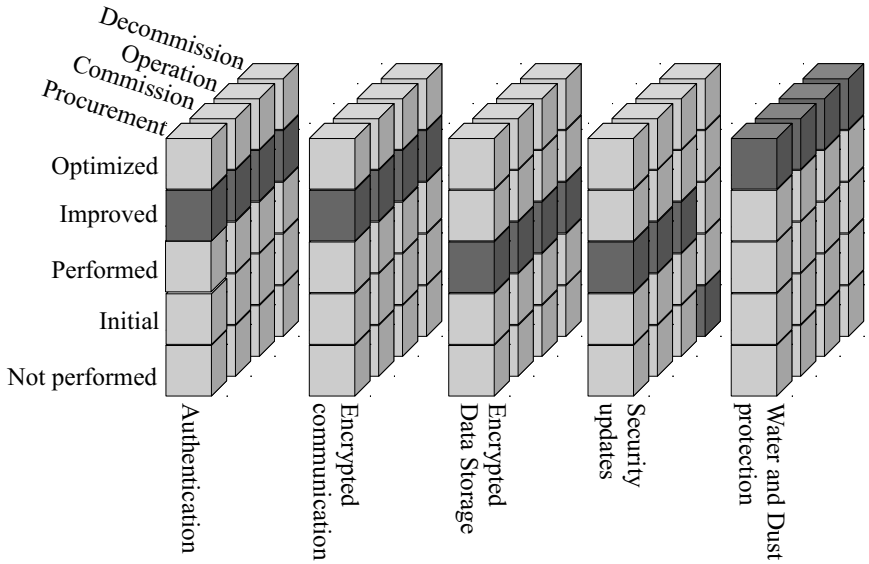

Fig. 1: Result: 4 MP Vandal WDR Fixed Dome Network Camera

We do these steps for all other 59 IoT devices. The documentation of the results is shown in Appendix A.

4.3 Data Analysis

In this section, we present the results of our evaluation and systematically answer the questions raised in the beginning of the evaluation.

The first question for our evaluation was, if it is possible to use INFINITE to evaluate the security of IoT devices with different application scenarios. In order to answer this question, it is useful to analyze how often each maturity level was reached within the device categories. Figure 2 illustrates these facts.

It can be clearly seen that the maturity level were reached with varying frequency within the device classes. The IoT devices of the class IoT smoke detector have reached maturity level 0 a total of 203 times. In comparison, maturity level 0 was only reached 169 times for the IoT Temperature Sensors. In the class IoT Security Cameras, maturity level 0 was reached a total of 81 times. Maturity Level 1 on the other hand was only reached 10 times for the IoT Security Cameras, 8 times for the IoT Temperature sensors and none for the IoT Smoke detectors. Differences can also be seen for maturity level 2. The class IoT Security Cameras have by far reached this maturity level most frequently. In the upper two maturity levels 3 and 4, all device classes perform similarly.

Figure 2 illustrates differences between the device classes by looking at the average achieved maturity level. For the security practice *water and dust protection* the IoT security cameras have reached

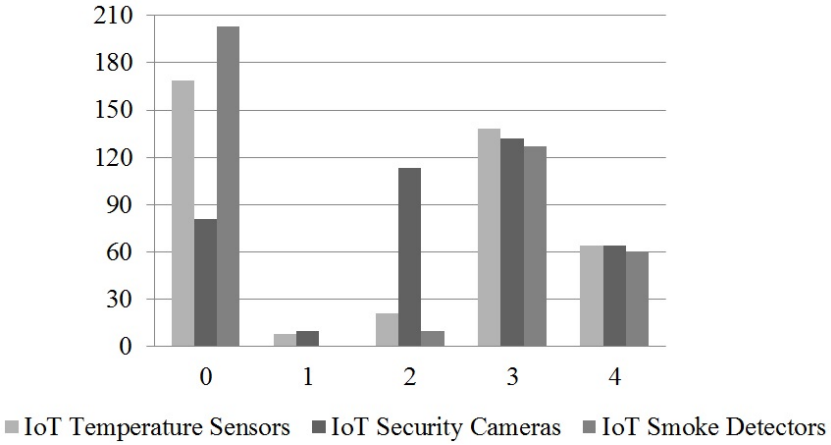

Fig. 2: Comparison of the Device Classes

maturity level 3,55 in average. This is by far the best result in compare to the IoT temperature sensors and the IoT smoke detectors. For the security practice *encrypted data storage*, all IoT device classes have achieved the worst results. However, the IoT security cameras are still the best with an average maturity level of 1,05. The other two IoT device classes achieved an average maturity level of 0.4. For the security practices *authentication* and *encrypted Communication*, the IoT smoke detectors have achieved the best results. For both security practices an average maturity level of 2,7 was achieved. The IoT security cameras have reached an average maturity level of 2,15 for the security practice *authentication*. This is the worst of all three device classes. Also for the security practice *security updates* the IoT security cameras have reached the worst result with an average maturity level of 1,75. The IoT temperature sensors are slightly better with an average maturity level of 1,9. The best result for was achieved by the IoT smoke detectors with an average maturity level of 2,06.

A comparison of the three device classes is possible, because the IoT devices have the same security requirements despite the different application scenarios. All devices of the three IoT device classes send private information over the internet. That means, security protocols are required to protect this communication. Furthermore, all IoT devices are operated with software. If vulnerabilities in the software become known, it must be possible to update the software on each device. The protection against water and dust also applies to all device classes. The sensitive sensors of all IoT devices can be damaged by the ingress of dust or water. Thus, the hardware of the IoT devices must be protected against this threats.

The second question for our evaluation was, if it is possible to use INFINITE to meaningfully evaluate the security of IoT devices with same application scenarios. To answer this question we can use Figure 2 again. It also includes the standard deviations for the security practices of each IoT device class. The standard deviation is represented by colored areas in the background. The standard deviations of the IoT security cameras across all security practices are between 0,800 and 1,268. For example, the average maturity level of 3,55 for the security practice *water and dust protection* of all IoT security

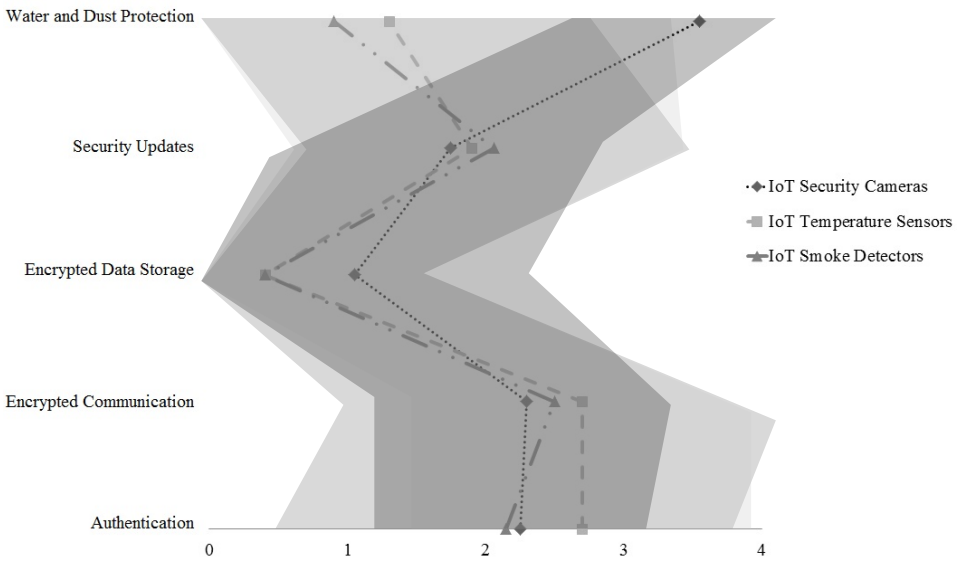

Fig. 3: Average Maturity Level For Each Device Class

cameras varies in average about 0,921. That indicates differences between the IoT security cameras for this certain security practice. However, same holds for the other security practices too. Each security practice has a standard deviation around one. For the IoT temperature sensors, the standard deviation is between 1,208 and 1,820 and for the IoT smoke detectors between 1,208, and 1,631. Thus, it is also possible to make a meaningful distinction for security properties between the IoT devices within the same IoT device class.

With our evaluation, we also want to find out, whether INFINITE can identify changes in the maturity level of a certain security practice over the life cycle. For the case study, we made some assumptions that makes it possible to evaluate the IoT devices equally. One of these assumptions is that authentication protocols like TLS or encryption algorithms like AES are available for the entire life cycle. Same holds for physical protection against water and dust. This assumption meant that there were no changes in the maturity level for four of the five security practices. Only for the security updates INFINITE was able to identify changes in the maturity level over the life cycle. Figure 4 illustrates the average maturity level for the security practice "*security updates* for all IoT device classes over the entire life cycle.

It can be clearly seen that security updates are available in every IoT device class at the beginning of the life cycle. The average maturity level remains constant until the operation phase for each IoT device class. No manufacturer has provided information on whether the IoT device will receive security updates for the entire life cycle. Some manufacturers only offered lifetime customer support. Due to this fact, the average maturity level for the security practice *security Updates* decreases in the final life cycle phase for all IoT device classes. That means, INFINITE is able to identify changes in

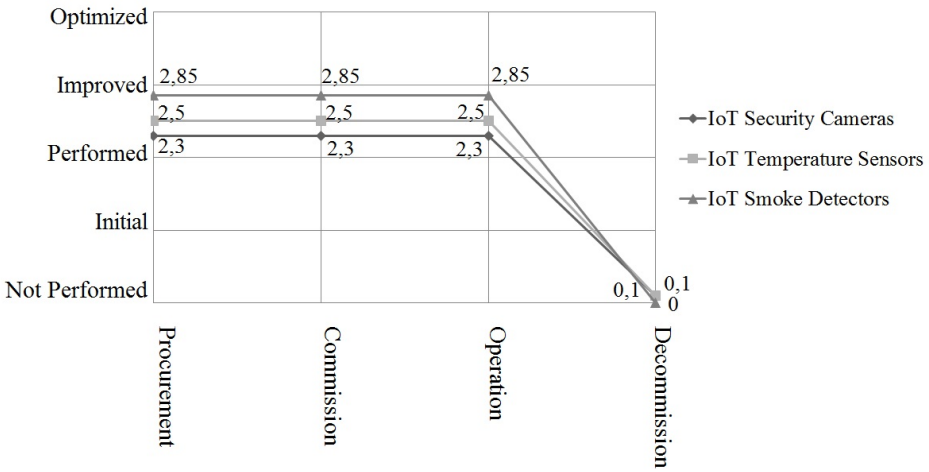

Fig. 4: Average Maturity Level for Security Updates over the life cycle

the maturity level over the life cycle. However, before purchasing an IoT device, it is not possible to identify a security practice that might be no longer available after a certain time due to a security update.

Furthermore, we were able to determine that it is not possible to obtain all information needed by INFINITE without contacting the manufacturer. Figure 5 illustrates, that most of the information about a security practice is available for the IoT security cameras. Each of the 20 manufacturers provides information about the *water and dust protection* of the IoT security camera. For 90% of the IoT security cameras, information about *encrypted communication* and *authentication* is provided by the manufacturer. Information about *security updates* is provided for 73,8%. Information about *encrypted data storage* with 45% is the least available for the IoT security cameras. For 85% of the IoT temperature sensors, information about *encrypted communication* and *authentication* is provided by the manufacturer. Information about *security updates* is provided for 73,8%. For 35,4% of the IoT temperature sensors, information about *water and dust protection* are available. For only 10% of the IoT temperature sensors, information about *encrypted data storage* is available. The least information was available for the IoT smoke detectors. Information about *encrypted communication* was available for 75,1%. Information about *security updates* is available with a similar percentage at 73,8%. For 65%, information about *authentication* is provided. For *water and dust protection* and *encrypted data storage*, as much information is available for the IoT smoke detectors as for the IoT temperature sensors.

The problem of missing information about the availability of a certain security practice can be solved, for example, by not procuring any IoT device that achieves the lowest maturity level for at least one security practice. As soon as an IoT device has reached the maturity level *initial* for a security practice, information is definitely available. A second option would be to contact the manufacturer directly.

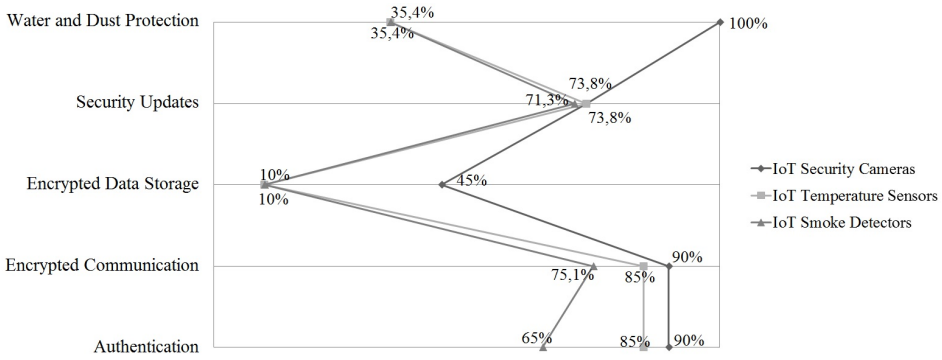

Fig. 5: Information Availability

Some manufacturers offer a FAQ section on their websites to answer customers questions. Otherwise there is also the possibility to contact the manufacturer by phone or e-mail.

Another question, we wanted to answer with our evaluation is, whether INFINITE can be used to identify IoT devices that comply with an organization's security policy. In our scenario, the drug manufacturer defined a policy that only IoT devices may be used on company premises, that complies with state of the art with regard to its security properties. To fulfill this policy, an IoT device has to reach at least maturity level three for each security practice and life cycle phase. Figure 6 illustrates in percentages how often the IoT devices of each IoT device class have reached maturity level three or higher. For the security practice *water and dust protection*, 80% of the IoT security cameras reached at least maturity level 3 or higher. This is by far the best result. Only 30% of the IoT temperature sensors and 20% of the IoT smoke detectors reached maturity level 3 or higher for this security practice. The IoT security cameras also achieved the best result for the security practice *security updates*. Overall 63,7%, reached maturity level three or higher. 52% of the IoT temperature sensors and only 30% of the IoT smoke detectors still met the specified policy. For the security practice *encrypted data storage*, all three IoT device classes achieved their worst results. However, the IoT security cameras are still the best IoT device class with 20%. Both the IoT temperature sensors and the IoT smoke detectors only reach 10%. For the security practice *encrypted communication*, the IoT security cameras and IoT temperature sensors met the security policy for 75%. With 70%, the IoT smoke detectors achieve the worst result for this security practice. The IoT temperature sensors achieved the best result for the security practice *authentication*. Overall, the policy was met for 70% of the IoT temperature sensors. With 65%, the IoT smoke detectors take second place for this security practice. The IoT security cameras achieved the worst result. Only 40% of the IoT security cameras reached maturity level 3 or higher.

In case an IoT device does not meet the security policy for one or more security practices, the reason should be identified. The first reason could be, the manufacturer provides information about a certain security practice and the IoT device still not meet the policy. That means, the IoT device does not meet the security policy for sure. In this case, the IoT device should not be procured. The second reason could be that the manufacturer does not provide information about the security practice. In this case,

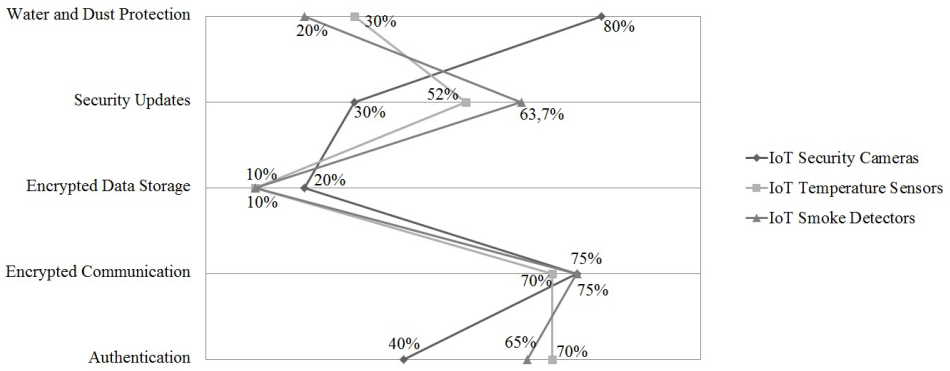

Fig. 6: Policy Fulfillment

it is not guaranteed that the IoT device does not meet the security policy. The manufacturers should be contacted to obtain the missing information. If the manufacturer confirms that the security practice is available for a certain degree, the use of the IoT device can be allowed. However, every company defines its individual security policy. So that INFINITE can be used for identifying IoT devices that comply with other organization's security policy, the policy must be defined in a way that it can be assigned to a certain maturity level. For more complex security policies, additional security practices can also be added to INFINITE. In this way, more specific security requirements for an IoT device can be evaluated. At the same time, this reduces the number of different application scenarios that can be evaluated with INFINITE. The more security practices are added for evaluation, the fewer application scenarios can be evaluated.

Clustering We also wanted to find out, if there are clusters of IoT devices with similar properties. Thus, we have used a clustering algorithm for all 60 IoT devices. We were particularly interested in whether INFINITE's evaluation results reveal different implementations of security practices over the life cycle. We have used the k-means clustering algorithm implemented in Weka, because this algorithm strives to identify groups with a small in-group variance. K-means needs the number of clusters to be identified. Thus, we have used the ellbow method. In particular, we have tested at which number of clusters the sum of the squared errors in the cluster assignment shows a „knee". As Figure 7 shows, there is a well-identifiable cut-off point at 4 clusters in the decrease of our error measure.

Since there is a sort order between the maturity level from 0 „not performed" to 4 *optimized*, we have considered the maturity level as numeric data. Table 8 shows the respective cluster assignment for four clusters $C0 \cdots C3$.

The largest cluster C0 includes 23 IoT devices from all three IoT device classes. All IoT devices except one are smoke detectors or temperature sensors. The cluster is characterized by devices having mostly implemented the security practices authentication, and encrypted communication and security updates on a maturity level *performed* or *improved*. Neither the security practice *water and dust protection* nor *encrypted data storage* was implemented. Based on this information, IoT devices in C0

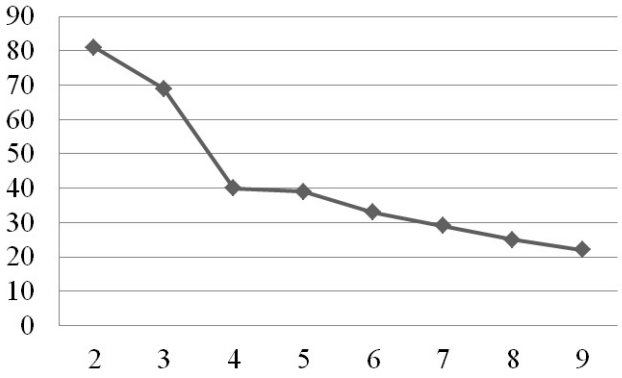

Fig. 7: Ellbow method

might be suitable for indoor environments without further security requirements. The second-largest cluster C1 includes 16 IoT devices. Approx. the half of them belonging to the IoT device class of IoT security cameras. In contrast to C0, the IoT devices in this cluster have also implemented the security practice *water and dust protection* on maturity level *improved* or *optimized*. That means, the IoT devices of cluster C1 are suitable for an outdoor usage. However, due to the fact that the security practice *encrypted data storage* is also *not implemented* or *initial*, the IoT devices should only be used in case there are no further security requirements. The third cluster C2 includes 12 IoT devices. The security practice *encrypted data storage* is added on maturity level *improved*. Two thirds of the IoT devices of this cluster are IoT security cameras. The IoT devices of cluster C2 have the highest security requirements compared to all other clusters. That means, these IoT devices can be used if certain security requirements have to be met for use. The smallest cluster C3 contains 9 IoT devices. These IoT devices rely on *security updates* level *performed* and weak *water and dust protection initial* and below. The majority of the devices in this cluster are smoke detectors and temperature sensors.

Tab. 8: Cluster assignment

	Cluster	*Full Data*	C0	C1	C2	C3
	Number of data sets	60	23	16	12	9
Security Practice / Phase						
Authentication	Procurement	2,4	2,7	2,8	2,9	0,0
Authentication	Installation	2,4	2,7	2,8	2,9	0,0
Authentication	Operation	2,4	2,7	2,8	2,9	0,0
Authentication	Decommission	2,4	2,7	2,8	2,9	0,0
Encrypted Communication	Procurement	2,6	3,0	3,1	3,1	0,0
Encrypted Communication	Installation	2,6	3,0	3,1	3,1	0,0
Encrypted Communication	Operation	2,6	3,0	3,1	3,1	0,0
Encrypted Communication	Decommission	2,6	3,0	3,1	3,1	0,0
Encrypted Data Storage	Procurement	0,6	0,0	0,1	3,0	0,0
Encrypted Data Storage	Installation	0,6	0,0	0,1	3,0	0,0
Encrypted Data Storage	Operation	0,6	0,0	0,1	3,0	0,0
Encrypted Data Storage	Decommission	0,6	0,0	0,1	3,0	0,0
Security Updates	Procurement	2,5	2,6	2,5	2,8	2,1
Security Updates	Installation	2,5	2,6	2,5	2,8	2,1
Security Updates	Operation	2,5	2,6	2,5	2,8	2,1
Security Updates	Decommission	0,1	0,0	0,0	0,1	0,2
Water and Dust Protection	Procurement	1,9	0,0	3,8	3,8	0,9
Water and Dust Protection	Installation	1,9	0,0	3,8	3,8	0,9
Water and Dust Protection	Operation	1,9	0,0	3,8	3,8	0,9
Water and Dust Protection	Decommission	1,9	0,0	3,8	3,8	0,9
	Security Camera	20	1	9	8	2
	Smoke Detector	20	11	3	2	4
	Temperature Sensor	20	11	4	2	3

As already observed, next to none of the devices in all clusters considers that sensitive data might be stored on a device after decommission, e.g., WLAN credentials, usernames, passwords or CCTV footage. To protect these data, security updates are still required after reaching the decommission phase.

5 Conclusion

This work was motivated by the fact that corporate customers are not able to evaluate the security of IoT devices. This is a big problem, because the security of IoT devices on the world market fluctuates greatly due to different legal requirements. Therefore, we introduced the 3-dimensional INternet oF thINgs maturITy modEl INFINITE. We defined the three axis of INFINITE IoT Life Cycle, IoT Security Practices and IoT Maturity Level and evaluated INFINITE through a case study with atotal of 60 IoT devices. Our evaluation has shown that INFINITE can be used to evaluate the security of IoT devices. The results can be used to compare the security of IoT devices with similar applications and also complete different applications. However, without manufacturers cooperation, it is difficult

for corporate customers to obtain all the information required to evaluate the security of an IoT device with INFINITE. With a clear security policy, defined by the companies management, INFINITE can also be used to find out, which security requirements an IoT device must fulfill to meet the security policy. This information can be used as a basis for an individualized IoT device for corporate customers. Furthermore, it is necessary to identify needed product properties of the IoT devices before using INFINITE.

A Appendix: Documentation

Tab. 9: IoT Security Cameras Documentation

ID	Security Practices				Notes
	Protocol	Encryption	Updates	protection	
Vandal WDR	SSL	RSA	manual	IP67	no updates in decommission
Eufycam 2C	SSL	AES128	automatic	IP67	no updates in decommission but lifetime support
Tapo C310 V1	TLS	AES128	automatic	IP66	no updates in decommission
Google Nest	SSL	AES128	automatic	IP65	no updates in decommission
5MP PTZ	SSL	RSA	automatic	weather proof	no updates in decommission
Laxihub O1	EAP	AES128	automatic	IP65	no updates in decommission
Arlo Ultra	TLS	AES128	automatic	water proof	no updates in decommission
IPC-HDBW5831E	TLS	RSA	automatic	IP67	no updates in decommission
D-Link H.265	SSL	RSA	automatic	IP66	no updates in decommission
Axis P1447	TLS	RSA	manual	IP66	no updates in decommission
WV-X8570N	SSL	RSA	manual	IP66	no updates in decommission
Cam IR	-	-	manual	IP65	no updates in decommission but lifetime support
IP Tube	TLS	RSA	manual	IP67	no updates in decommission
LUPUS-LE281	SSL	RSA	manual	IP66	no updates in decommission
H.264 960P	-	-	-	water proof	-
IP9165-HP	SSL	RSA	manual	-	no updates in decommission, water proof case can be purchased
DS-2CD2025FWD	SSL	RSA	manual	IP67	no updates in decommission
IPC-B650H-Z	SSL	RSA	manual	IP67	no updates in decommission
Cisco Video	SSL	RSA	manual	IP66	no updates in decommission
Smart Outdoor Cam	-	-	manual	certified protection	uses end to end encryption but no protocols are mentioned

Tab. 10: IoT Temperature Sensors Documentation

ID	Security Practices				Notes
	Protocol	Encryption	Updates	protection	
Aqara Temp. Sensor	AES in CCM	AES128	manual	IP20	no updates in decommission
SONOFF SNZB-02	AES in CCM	AES128	automatic	-	no updates in decommission
ELV HmIP-WTH-2	HomematicIP	HomematicIP	automatic	IP20	no updates in decom., Homematic IP is certified
RSH Temp. Sensor	AES in CCM	AES128	automatic	-	no updates in decommission
Nous E6	AES in CCM	AES128	support	-	not a life time support
Temp. Reader	AES in CCM	AES128	support	-	life time support not sure, prot. are certified
Long Range Sensor	TLS	AES128	manual	certified prot.	no updates in decommission
Shelly H&T	TLS	AES128	automatic	-	no updates in decommission
Zemismart Sensor	AES in CCM	AES128	automatic	-	no updates in decommission
Tesla Sensor	AES in CCM	AES128	automatic	-	no updates in decommission
Wireless Sensor	-	-	automatic	IP68	end to end encr. but no protocols are mentioned
Govee Hygrometer	-	-	automatic	-	No updates in decom. but lifetime support
Frient Sensor	AES in CCM	AES128	automatic	IP20	no updates in decom., protocols are certified
Bosch Thermostat	TLS	AES128	automatic	IP20	no updates in decom., protocols are certified
Temperature Logger	-	-	-	-	-
Climate Sensor	AES in CCM	AES128	automatic	-	no updates in decommission
Smart Home 400	AES in CCM	AES128	automatic	-	no updates in decommission
Proteus AMBIO	-	-	manual	different conditions	no updates in decommission
Multi.Sensor	AES in CCM	AES128	automatic	-	no updates in decommission
Bresser Hygrometer	EAP	AES128	automatic	-	no updates in decommission

Tab. 11: IoT Smoke Detectors Documentation

ID	Security Practices				Notes
	Protocol	Encryption	Updates	protection	
Gigaset	AES in CCM	AES128	automatic	-	no updates in decommission
Banggood	-	-	automatic	-	no updates in decommission
LH-601WF	AES in CCM	AES128	automatic	-	no updates in decommission
PA-443W	-	-	automatic	-	no updates in decommission
HS1SA	AES in CCM	AES128	-	-	protocols are certified
Wi-Fi Smoke Detector	-	-	automatic	-	no updates in decommission
Frient Smoke Alarm	AES in CCM	AES128	automatic	IP20	no updates in decom. protocols are certified
ABUS Detector	-	AES128	automatic	-	no updates in decommission
HmIP-SWSD	HomematicIP	HomematicIP	automatic	IP20	no updates in decom. protocols are certified
Bosch Smoke Alarm	TLS	AES128	automatic	IP20	no updates in decom. protocols are certified
Anka Smoke Alarm	AES in CCM	AES128	automatic	-	no updates in decommission
SH8-99101UK	-	-	automatic	IP20	no updates in decom., communication is trusted and encrypted, no prot. mentioned
R7049	AES in CCM	AES128	automatic	-	no updates in decommission
Photoel. Detector	-	AES128	manual	-	no updates in decommission
DWL-2600AP	EAP	AES128	manual	-	no updates in decom., certified use of EAP (IEEE 802.1X)
Nedis Detector	-	-	automatic	-	no updates in decommission
Zemismart Sensor	AES in CCM	AES128	automatic	dust proof	no updates in decommission
Fibaro Sensor	-	AES128	automatic	-	no updates in decommission
ELRO Connects	EAP	AES128	automatic	-	no updates in decommission
PSG01	-	AES128	automatic	-	no updates in decommission

References

[AB22] ABUS August Bremicker Söhne KG: ABUS Z-Wave Smoke Detector, https://www.abus.com/eng/content/view/full/59249, Accessed February 2022, 2022.

[Ae21] Aeotec Technology Co., Ltd.: Where to buy Aeotec Multipurpose Sensor, https://aeotec.com/smartthings/zigbee-multipurpose-sensor.html, Accessed February 2022, 2021.

[Ah17] Ahmed, A. W.; Ahmed, M. M.; Khan, O. A.; Shah, M. A.: A comprehensive analysis on the security threats and their countermeasures of IoT. International Journal of Advanced Computer Science and Applications 8/7, pp. 489–501, 2017.

[Al20] Alladi, T.; Chamola, V.; Sikdar, B.; Choo, K.-K. R.: Consumer IoT: Security Vulnerability Case Studies and Solutions. IEEE Consumer Electronics Magazine 9/2, pp. 17–25, 2020.

[Al22] Allterco Robotics Ltd.: Shelly H&T, https://shelly.cloud/knowledge-base/devices/shelly-ht/, Accessed February 2022, 2022.

[An22a] Anka Sci-tech Co., Ltd.: Zigbee Smoke alarm, https://www.anka-security.com/product/zigbee-smoke-alarm/, Accessed February 2022, 2022.

[An22b] Anker Technology (UK) Ltd.: eufyCam 2C, https://uk.eufylife.com/products/t88313d2 Accessed February 2022, 2022.

[Ar20] Arenti Europe B.V.: O1 Outdoor Weather-Proof Wi-Fi Bullet Camera, https://www.laxihub.com/collections/outdoor-indoor/products/o1-outdoor-wi-fi-camera Accessed February 2022, 2020.

[Ar21] Arlo Technologies Inc.: Arlo Ultra, https://www.arlo.com/en_gb/cameras/arlo-ultra Accessed February 2022, 2021.

[Ba21] Banggood Tchnology Co., Ltd.: WiFi Smoke Detector Fire Protection Portable Smoke Detector Home Safe Security Smoke Alarm Sensor TUYA APP Smart Home, https://www.banggood.com/WiFi-Smoke-Detector-Fire-Protection-Portable-Smoke-Detector-Home-Safe-Security-Smoke-Alarm-Sensor-TUYA-APP-Smart-Home-p-1829007.html, Accessed February 2022, 2021.

[BH20] Buchmann, E.; Hartmann, A.: Identifying Long-Term Risks of the Internet of Things. UBICOMM 2020: The Fourteenth International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies/, 2020.

[Br21] Bresser GmbH: Bresser Tuya Smart Thermo- / Hygrometer, https://www.bresser.de/en/Weather-Time/Weather-Stations/BRESSER-Tuya-Smart.html, Accessed February 2022, 2021.

[CAW10] Caralli, R. A.; Allen, J. H.; White, D. W.: CERT resilience management model (CERT-RMM): a maturity model for managing operational resilience. Addison-Wesley Professional, 2010.

[Ch21] China Security & Fire IoT Sensing Co., Ltd.: Smoke Sensor LH-601WF, http://www.ihorn-tech.com/anti-theft/alarm-accessories/detail_240.html, Accessed February 2022, 2021.

[Ci13] Cisco Systems, Inc.: Cisco Video Surveillance PTZ IP Cameras, https://www.cisco.com/c/en/us/support/physical-security/video-surveillance-ptz-ip-cameras/series.html, Accessed February 2022, 2013.

[Cl21] Closed Circuit Television Camera Pros LLC.: Vandal-Proof Dome Cameras, https://www.cctvcamerapros.com/Vandal-Proof-Dome-Cameras-s/642.htm, Accessed November 2021, 2021.

[CMS15] Curtis, P.; Mehravari, N.; Stevens, J.: Cybersecurity capability maturity model for information technology services (c2m2 for it services), version 1.0, tech. rep., Carnegie-Mellon Univ. Pittsburgh pa Pittsburgh United States, 2015.

[Co20] CoSa Connects Ltd.: ELRO Connects K1 Smoke Detector Kit (SF400S), https://www.elro.eu/en/elro-connects-k1-smoke-detector-kit-sf400s, Accessed February 2022, 2020.

[Da21] Dahua Technology Co., Ltd: IPC-HDBW5831E-Z5E, https://www.dahuasecurity.com/mena/products/All-Products/Network-Cameras/Pro-Series/8-MP/IPC-HDBW5831E-Z5E Accessed February 2022, 2021.

[Di22] Disruptive Technologies: Wireless Temperature Sensor, https://www.disruptive-technologies.com/products/wireless-sensors/wireless-temperature-sensor, Accessed February 2022, 2022.

[DL20] D-Link (Europe) Ltd.: Unified Wireless N PoE Access Point DWL-2600AP, https://eu.dlink.com/uk/en/products/dwl-2600ap-unified-wireless-n-poe-access-point#support, Accessed February 2022, 2020.

[Do22] Dongguan Daying Electronics Technology Co., Ltd.: Wi-Fi Smoke Detector, http://www.dygsm.com/Products_detail.asp?id=80, Accessed February 2022, 2022.

[DS21] DSM&T Company Inc.: IP Rating Chart, https://www.dsmt.com/resources/ip-rating-chart/, Accessed November 2021, 2021.

[Dy20] Dynamode Inc.: Smart Home 400 Temperature & Humidity Sensor, http://www.dynamode.net/english/pages/product/Smart%20Home/Smart%20Kit/WL-400-THSH.html, Accessed February 2022, 2020.

[El18] Elijah, O.; Rahman, T. A.; Orikumhi, I.; Leow, C. Y.; Hindia, M. N.: An overview of Internet of Things (IoT) and data analytics in agriculture: Benefits and challenges. IEEE Internet of Things Journal 5/5, pp. 3758–3773, 2018.

[EL21a] ELV Elektronik AG: ELV Bausatz Homematic IP Wandthermostat HmIP-WTH-2 mit Luftfeuchtigkeitssensor für Smart Home, https://de.elv.com/elv-homematic-ip-komplettbausatz-wandthermostat-hmip-wth-2-fuer-smart-home-hausautomation-153698, Accessed February 2022, 2021.

[EL21b] ELV Elektronik AG: Homematic IP Smart Home 3er Set Rauchwarnmelder HmIP-SWSD mit 10-Jahres-Lithium-Batterie, https://de.elv.com/homematic-ip-rauchmelder-hmip-swsd-mit-10-jahres-lithium-batterie-3er-set-128715?fs=3420603391, Accessed February 2022, 2021.

[EX21] EXPERT-Security GmbH & Co. KG: Axis P1447-LE IP-Kamera 5MP T/N IR PoE IP67 IK10, https://www.expert-security.de/axis-p1447-le-ip-kamera-5mp-t-n-ir-poe-ip67-ik10.html Accessed February 2022, 2021.

[Fe19] Federal Office for Information Security: BSI IT Grundschutz Compendium Edition 2019. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-it-gs-comp-2019.pdf, Accessed November 2021/, 2019.

[FI22] FIBAR GROUP S.A.: Smoke Sensor, https://www.fibaro.com/en/products/smoke-sensor/, Accessed February 2022, 2022.

[Fr22a] Frient: Intelligent Smoke Alarm, https://frient.com/products/intelligent-smoke-alarm/, Accessed February 2022, 2022.

[Fr22b] Frient: Smart Humidity Sensor, https://frient.com/products/smart-humidity-sensor/, Accessed February 2022, 2022.

[Gi21] Gigaset Communications GmbH: Gigaset Smoke Sensor 2.0 ONE X, https://www.gigaset.com/de_de/gigaset-smoke-sensor-2-0-one-x/, Accessed February 2022, 2021.

[Go21] Google Ireland Ltd.: Nest Cam outdoor or indoor, battery, https://store.google.com/us/product/nest_cam_battery Accessed February 2022, 2021.

[Go22] Govee: Govee Wi-Fi Thermo-Hygrometer, https://us.govee.com/products/wi-fi-temperature-humidity-sensor, Accessed February 2022, 2022.

[Ha21] Hangzhou Hikvision Digital Technology Co., Ltd.: 4 MP Vandal WDR Fixed Dome Network Camera, https://www.hikvision.com/de/products/IP-Products/Network-Cameras/Pro-Series-EasyIP-/ds-2cd2143g2-i-s-/ Accessed February 2022, 2021.

[Ha22a] Hangzhou Hikvision Digital Technology Co., Ltd.: Wireless Photoelectric Smoke Detector, https://www.hikvision.com/en/products/Alarm-Products/Hikvision-Intrusion-Detector/Wireless-Detector/ds-pdsmk-s-we/, Accessed February 2022, 2022.

[Ha22b] Hangzhou Konke Information Technology Co., Ltd.: Temperature and Humidity Reader, https://www.konkesmart.com/sensor/temperature-and-humidity-sensor/temperature-and-humidity-reader.html, Accessed February 2022, 2022.

[Hi16] Hikvision Digital Technology Co., Ltd.: Hikvision, https://hiwatch.de/wp-content/uploads/2019/07/DS-2CD2025FWD-I-DE.pdf, Accessed February 2022, 2016.

[HR20] Hessel, S.; Reusch, P.: Legal requirements for IoT security in Europe: current state and outlook, https://www.ibanet.org/article/76DE516B-CAFD-4596-B354-9A2E14F2EEC4, Accessed November 2021, 2020.

[In13a] International Business Machines Corporation 2013: Using the IBM Security Framework and IBM Security Blueprintto Realize Business-Driven Security, http://www.redbooks.ibm.com/redbooks/pdfs/sg248100.pdf, Accessed November 2021, 2013.

[In13b] International Organization for Standardization: Information technology - Security techniques - Information security management systems - Requirements, https://www.iso.org/standard/54534.html, Accessed November 2021, 2013.

[In16] Inkovideo GmbH & Co. KG: HiLook IPC-B650H-Z, https://hilook.de/hilook-b650hz-poe-ueberwachungskamera.html, Accessed February 2022, 2016.

[iP21] i-PRO UK Ltd.: WV-X8570N, https://i-pro.com/eu/en/surveillance/products/wv-x8570n Accessed February 2022, 2021.

[IT20] IT Security Association Germany: IT Security Act (Germany) and EU General Data Protection Regulation: Guidline State of the art, https://www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/, Accessed November 2021, 2020.

[Ka21] Kaspersky Lab.: Best Practices for IoT Security, https://www.kaspersky.com/resource-center/preemptive-safety/best-practices-for-iot-security, Accessed November 2021, 2021.

[Ki22] KingKees B.V.: R7049 Smoke Alarm Single Unit, https://wooxhome.com/products-c10/security-c6/r7049-smoke-alarm-single-unit-p70, Accessed February 2022, 2022.

[Kk16] Kkmoon SA: KKmoon H.264 960P 2.8-12mm Auto-focus PTZ IR-Cut Waterproof WiFi Camera, https://www.kkmoon.com/p-s600-eu.html, Accessed February 2022, 2016.

[Ko17] Kolias, C.; Kambourakis, G.; Stavrou, A.; Voas, J.: DDoS in the IoT: Mirai and other botnets. Computer 50/7, pp. 80–84, 2017.

[LE20] LED Innovation Perofmance Technik: SONOFF S55 Wi-Fi Smart Waterproof Socket, https://www.lip-technik.com/SONOFF-S55-Wi-Fi-Smart-Waterproof-Socket, Accessed November 2021, 2020.

[LH17] Le, N. T.; Hoang, D. B.: Capability maturity model and metrics framework for cyber cloud security. Scalable Computing/, 2017.

[Lo19] Lovells, H.: Privacy, Cybersecurity, and the Internet of Things in Asia: What to Expect in 2019, https://www.lexology.com/library/detail.aspx?g=c7293067-844f-4f90-88e1-7ddf3f413483, Accessed November 2021, 2019.

[Lu21a] Lumi United Technology Co., Ltd.: Temperature and Humidity Sensor, https://www.aqara.com/us/temperature_humidity_sensor.html, Accessed February 2022, 2021.

[Lu21b] Lupus Electronics: LUPUS - LE281 PoE, https://www.lupus-electronics.de/shop/en/Video-surveillance/Network-Cameras/PTZ-Cameras/LUPUS-LE281-PoE-p.html, Accessed February 2022, 2021.

[Mi21] Microsoft: Security best practices for Internet of Things (IoT), https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-best-practices, Accessed November 2021, 2021.

[Na20] Nation Institute of Standards and Technology: NIST Releases Draft Guidance on Internet of Things Device Cybersecurity, https://www.nist.gov/news-events/news/2020/12/nist-releases-draft-guidance-internet-things-device-cybersecurity, Accessed November 2021, 2020.

[Na21] National Control Devices LLC.: IoT Long Range Wireless Temperature Humidity Sensor, https://store.ncd.io/product/industrial-long-range-wireless-temperature-humidity-sensor/, Accessed February 2022, 2021.

[Ne16] Netatmo: Smart Outdoor Camera, https://www.netatmo.com/en-gb/security/cam-outdoor, Accessed February 2022, 2016.

[Ne20a] Nedis B.V.: Smart Climate Sensor, https://nedis.co.uk/en-gb/product/smart-home/climate/monitoring/550726063/smart-climate-sensor-zigbee-30-battery-powered-android-ios-white, Accessed February 2022, 2020.

[Ne20b] Nedis B.V.: SmartLife Smoke Detector, https://nedis.co.uk/en-gb/product/security-safety/home-prevention/smoke-detection/550691451/smartlife-smoke-detector-wi-fi-battery-powered-sensor-life-cycle-10-year-en-14604-max-battery-life-24-months-android-ios-85-db-white, Accessed February 2022, 2020.

[No22] Nous Corporation Ltd.: Smart ZigBee LCD Temperature and Humidity Sensor Nous E6, https://nous.technology/product/e6.html, Accessed February 2022, 2022.

[Ph21] Philio Technology Corporation, Inc.: PSG01 Z-wave smoke detector, https://www.zwavetaiwan.com.tw/psg01, Accessed February 2022, 2021.

[Po16] Porambage, P.; Ylianttila, M.; Schmitt, C.; Kumar, P.; Gurtov, A.; Vasilakos, A. V.: The Quest for Privacy in the Internet of Things. IEEE Cloud Computing 3/2, pp. 36–45, 2016.

[Pr21] Proteus Sensors LLC.: Proteus AMBIO - Wireless Temperature/ Humidity Sensor, https://proteussensor.com/wireless-wifi-temperature-sensor.html, Accessed February 2022, 2021.

[Re21] Reolink Digital Technology Co., Ltd.: Smart 5MP PTZ WiFi Camera with Motion Spotlights, https://reolink.com/fi/product/e1-outdoor/ Accessed February 2022, 2021.

[Ro22a] Robert Bosch Smart Home GmbH: Room thermostat, https://www.bosch-smarthome.com/uk/en/products/devices/room-thermostat/, Accessed February 2022, 2022.

[Ro22b] Robert Bosch Smart Home GmbH: Smoke Alarm, https://www.bosch-smarthome.com/uk/en/products/devices/smoke-alarm/, Accessed February 2022, 2022.

[ROL18] Rahman, L. F.; Ozcelebi, T.; Lukkien, J.: Understanding IoT systems: a life cycle approach. Procedia computer science 130/, pp. 1057–1062, 2018.

[Se20] Selimis, G.; Wang, R.; Maes, R.; Schrijen, G.-J.; Münzer, M.; Ilić, S.; Willems, F. M.; Kusters, L.: RESCURE: A security solution for IoT life cycle. In: Proceedings of the 15th International Conference on Availability, Reliability and Security. Pp. 1–10, 2020.

[Sh16] Shenzhen Heiman Technology Co., Ltd.: Smart Smoke Sensor HS1SA, http://www.heimantech.com/product/?type=detail&id=3, Accessed February 2022, 2016.

[Sh20] Shandong Renke Control Technology Co.,Ltd.: Wifi temperature and humidity data logger, https://www.renkeer.com/product/wifi-temperature-and-humidity-data-logger/, Accessed February 2022, 2020.

[SKG19] Shoukry, A.; Khader, J.; Gani, S.: Improving business process and functionality using IoT based E3-value business model. Electronic Markets/, pp. 1–10, 2019.

[Sm22] Smartwares B.V.: Homewizard SH8-99101UK Smoke detector set, https://www.smartwares.eu/en-gb/smartwares-products/smarthome/smarthome-pro/homewizard-sh8-99101uk-smoke-detector-set-sh8--99101uk, Accessed February 2022, 2022.

[So18] Soós, G.; Kozma, D.; Janky, F. N.; Varga, P.: IoT Device Lifecycle – A Generic Model and a Use Case for Cellular Mobile Networks. In: 2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud). Pp. 176–183, 2018.

[SO21] SONOFF Technologies Co., Ltd: SONOFF SNZB-02 ZigBee Temperature & Humidity Sensor, https://sonoff.tech/product/smart-home-security/snzb-02/, Accessed February 2022, 2021.

[Sw17] Swanson, M. , Bartol, N. , Sabato, J. , Hash, J. and Graffo, L.: Security Metrics Guide for Information Technology Systems. https://www.nist.gov/publications/security-metrics-guide-information-technology-systems, Accessed November 2021/, 2017.

[SZ20] SZ PGST Co.,Ltd.: Tuya Intelligent WiFi Strobe Smoke Detector PA-443W, http://www.cn-pgst.com/Products/Intelligent_Fire_Alarm_System/Smoke_Detectors/124.html, Accessed February 2022, 2020.

[TE22] TESLA Solar, s.r.o.: Tesla Smart Sensor Temperature and Humidity, https://www.teslasmart.com/en/products/smart-sensors/tesla-smart-sensor-temperature-and-humidity/, Accessed February 2022, 2022.

[TP22] TP-Link Corporation Ltd.: Outdoor Security Wi-Fi Camera, https://www.tp-link.com/en/home-networking/cloud-camera/tapo-c310/#overview Accessed February 2022, 2022.

[Tu22] Tuya Inc.: RSH Tuya Smart Life Zigbee Temperature Sensor Humidity Detector Hygrometer Thermometer Support Alexa Google SmartThings, https://expo.tuya.com/product/953002, Accessed February 2022, 2022.

[Va21] Vacoslabs: Vacos Cam IR, https://www.vacos.com/products/vacos-cam-ir Accessed February 2022, 2021.

[VI16] VIVOTEK Inc.: IP9165-HP, https://www.vivotek.com/ip9165-hp#specifications, Accessed February 2022, 2016.

[YMF20] Yousefnezhad, N.; Malhi, A.; Främling, K.: Security in product lifecycle of IoT devices: A survey. Journal of Network and Computer Applications/, p. 102779, 2020.

[Ze22a] Zemismart: Tuya Zigbee Temperature and Humidity Sensor with LCD Screen Display Works With Amazon Google Home Assistant, https://www.zemismart.com/products/hs001, Accessed February 2022, 2022.

[Ze22b] Zemismart: Zemismart Tuya Zigbee Smart Smoke Sensor Smart Home Device Surveillance Wireless Smoke Detector, https://www.zemismart.com/products/zm-sm100-kgty, Accessed February 2022, 2022.