Long-Term Risks of IoT Devices: The Case of the Smart Fridge

Erik Buchmann[a,b]

[a] Dept. of Computer Science, Leipzig University, Germany
[b] Center for Scalable Data Analytics and Artificial Intelligence Dresden/Leipzig, Germany
Email: `buchmann@informatik.uni-leipzig.de`

Abstract—Replacing conventional devices with smart ones has many advantages, e.g., a seamless integration of physical objects into the user's digital environment or improved modes of use. However, if a conventional device is replaced by a smart device, its IT components can cause risks, that shorten the life of the device. Such risks stem from different life cycles of embedded soft- and hardware, libraries and protocols used, and the IT ecosystem required. This is problematic, because many conventional household appliances, say, a fridge or TV, have a much longer life span than typical IT equipment. In this paper, we use a systematic approach to identify long-term risks for the operational life span of a smart fridge. In particular, we identify 8 different use cases of three typical smart fridges, e.g., cooling or managing "best before" dates. We model the IT ecosystem needed to run these use cases, and we inspect each asset in this ecosystem for potential long-term risks. We found that even cooling, the most basic use case, is at risk in the long run. This is because the setting cooling parameters may depend on parts of the IT ecosystem that are not under the user's control. On the other hand, we did not find any risk that may lead to harm of the category "threatening". Our findings on the smart fridge can be generalized to other smart devices easily.

Keywords—Internet of Things; Security; Risk Management

I. INTRODUCTION

Advances in hard- and software have led to the trend to add sensors, computational resources and communication interfaces to traditional consumer products, and to connect them over the Internet to cloud services where an artificial intelligence approach interprets voice commands or enhance user experience. Together, such smart devices form the Internet of Things (IoT) [1]. In many cases, smart devices stem from non-smart predecessors. For example, a modern smart refrigerator looks and feels much like a classic non-smart refrigerator with some extras, e.g., remote control and expiration management for perishable foods.

Smart devices allow consumers to create smart homes with devices that can be controlled remotely via smartphone, adapt to the user's habits, and provide convenient services locally or on the Internet. However, media provide evidence that smart devices might come with operational risks that occur well after the time of purchase. With a familiar non-smart device in mind, customers may not expect risks like Examples 1-3, when choosing a smart device.

Example 1: *The software of a smart device may have an operational life-span that is much shorter than the life-span of its hardware [2]. For example, without regular functional and security updates, a smart TV soon becomes useless [3].*

Example 2: *Smart devices may be tied to a cloud service. For example, after a third-party service provider ceased its business, tens of thousands smart Internet radios became non-functional [4] without warning in advance.*

Example 3: *Changes in the legislation may prohibit the use of smart devices after years of operation. In Germany, for example, a child's smart toy [5] has been forbidden as a spying tool, three years after it had been introduced to the market, because it was not visible that the toy sends voice recordings into the cloud.*

In order to make smart devices accessible for risk management, a comprehensive catalog of potential risks is required. It is challenging to find a research method that delivers such a catalog. For example, the results of a study [6] depend on the insights of the study participants.

In this paper, we use smart fridges as a use case to compile a comprehensive set of long-term risks that are (a) specific for the smart fridge, i.e., do not exist for conventional fridges, and (b) may materialize years after the fridge has been purchased. We define our problem statement as follows:

Which specific risks for the continued long-term use of a smart fridge may appear after purchase, but cannot be expected from a conventional fridge?

We call a fridge a "smart fridge", if it contains computational capabilities and data links, which are not essential for the primary function "cooling food products". By "long-term", we refer to an operational life of >10 years, which can be expected from a fridge's hardware [7]. Intuitively, this may be the expectation of a customer replacing a broken fridge.

In this paper, we adapt our research method from [8] to methodically derive such long-term risks for a smart fridge in a domestic environment. We have identified *compliance risks* resulting from changing local, national or international rules, *economic risks* from future business decisions of the organizations involved, and *operational risks* considering the technical perspective of operating a smart fridge together with its IT ecosystem for more than 10 years. Due to our methodical approach, we consider our set of risks to be complete for this application scenario. We think that it can be easily adapted to similar scenarios.

The paper is structured as follows: In Section II, we briefly review related work. In Section III, we sketch our approach to identify long-term risks of smart fridges. In Section IV, we use this approach to obtain our set of risks. Section V concludes.
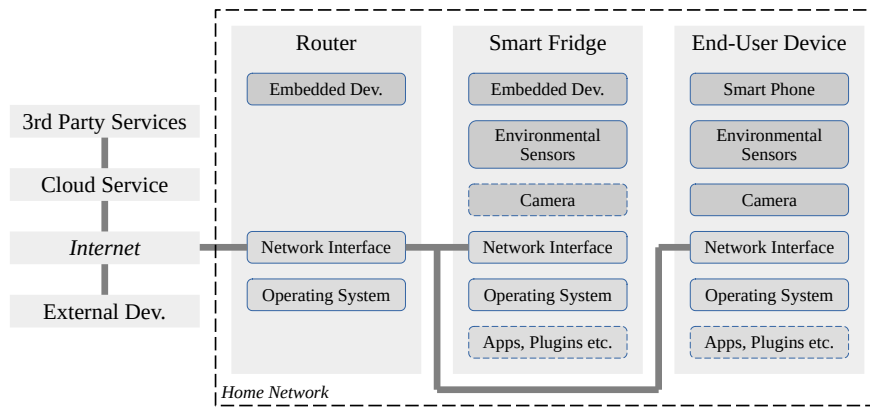
Figure 1. IT Architecture

II. RELATED WORK

This section summarizes methods, standards and findings related to our work. **Design science research** [9] is a method to design an artefact from a knowledge base, and evaluate and improve it in several rounds. Each round is divided into three cycles: The *relevance cycle* specifies and refines the use cases needed to construct the artefact and evaluate its applicability. The *rigor cycle* builds a knowledge base from literature and experience that is needed to evaluate the novelty and the research contribution of the artefact. The central *design cycle* iterates between building and evaluating the artefact, based on information from the other cycles.

The **BSI-Standard 200-3** [10] is based on IT-Grundschutz. It defines a process that allows organizations to assess their information security risks. In particular, the standard describes how to identify, classify, consolidate, assess and treat risks. Our concern is risk identification. In this respect, the standard distinguishes risks that arise from *elementary threats*, e.g., fire, theft, misconfiguration or manipulation, and *specific threats* from specific use cases. The risk identification starts with the modelling of the use cases. The risk catalog is then compiled from the consolidated risks of the individual IT assets, which are part of the model.

Advances in technology call for **risk analyses** before adoption. However, risk analyses typically use a descriptive research approach, focus on the current situation and/or have a narrow perspective, e.g., on current IT security or return on investment. For example, [11] reviews vulnerabilities of smart devices in the consumer market. The risk assessment approach in [12] considers the management of risk over the past two years, but does not project into the future, e.g., when security breaches remain untreated for a discontinued product. A study [6] provides a holistic view on future IoT risks, but a standardized questionnaire cannot provide a complete overview on future risks. In consequence, existing approaches that deal with IoT risks during the operational life of the device [13] [14] do not consider that vendors may loose interest in supporting discontinued products, or that it will be hard to find experts to maintain outdated technology. [2] uses threat models to assess risks due to discontinued services,

breaking updates, trade conflicts, etc., but it remains unclear if this risk assessment is exhaustive for the devices in question. In [8], we have defined a research method to identify long-term risks that are specific for smart devices. Because this method is fundamental for our paper, we will explain it in more detail in the next section.

The **long-term preservation of digital goods** has been extensively discussed [15] in the past years. The risks for digital content [16] overlap with the risks of using an outdated smart device in a modern environment. Examples are media obsolescence and format obsolescence [16], i.e., the digital object cannot be read with current devices due new media or new formats. Security properties have been established with protocols that are insecure now [17]. Digital objects, such as dynamic web pages [18] or computer games [19], require a complex execution environment.

III. HOW TO IDENTIFY LONG-TERM IoT RISKS

In this section, we briefly describe our research method, which we have developed in [8]. Our method adapts BSI-Standard 200-3 [10] so that it creates the knowledge base and designs a risk catalog that fits into relevance and design cycle of Design Science Research [9]. We use research literature to foster the rigor cycle.

For this paper, we have extended two aspects of [8]: We explicitly refer to an operational scenario (in our case: a domestic environment) to assess the extent of potential harms and damages. Furthermore, we do not add assets to our infrastructure model that do not add specific risks for the smart device in question, e.g., the Internet router or the electricity supplier. In particular, we use the following steps:

1) Select typical devices and identify the use cases for these devices in a given scenario. Model its IT infrastructure.
2) Determine under which conditions each asset in this infrastructure operates as intended by the use cases.
3) Append this condition to the risk set, if it is not present at purchase and doesn't exist for non-smart devices.
4) Assess the harm the risks could cause, and consolidate risks that are identical for multiple assets.
5) Back up each individual risk by literature.

IV. LONG-TERM RISKS OF A SMART FRIDGE

In this section, we apply our research method from Section III to identify a comprehensive set of long-term risks associated with smart fridges.

Operational scenario: We base our analysis on a domestic environment, where the fridge stores perishable food that needs cooling and has a limited economic value. The user of the fridge values the user experience more than privacy and likes to use all technical possibilities of the digital services offered by the smart fridge. The user can be expected to detect spoiled food, but does not possess the IT-security knowledge needed to detect cyber attacks on the smart fridge. Figure 1 illustrates the IT architecture for this scenario.

A. Device Selection and Use Cases

According to Step 1 of our research method, we select three typical devices from the category "Smart Fridge":

1) Bosch KGN36HI32
2) Samsung RF27T5501SG
3) LG GSX960NEAZ

The Bosch KGN36HI32 can be controlled via the Bosch Home Connect platform, which connects to Amazon Alexa and other voice assistants and sends temperature alarms to the user's smartphone. It is equipped with internal cameras, that monitor the cooled food products. The Samsung RF27T5501SG provides similar technical features as the Bosch fridge, but uses the Samsung product family: It contains a Samsung Family Hub and connects to a voice assistant called Bixby. In addition, it provides a large LCD screen with apps and Internet access via WLAN, and an ice dispenser. The LG GSX960NEAZ provides the smallest set of smart features: It only controls fridge parameters and functions, such as defrost and alerts, via LG smartphone app. But it does not contain cameras, smart home hubs or LCD screens.

TABLE I. CATEGORIES OF USE CASES

Id	Name	Description
U1	Cooling	Storing and cooling food products.
U2	Monitoring	Monitoring the food storage via camera.
U3	Management	Managing food expiration and shopping lists.
U4	Shopping	Replenish food storage.
U5	Multimedia	Playing music, TV streams, Internet access.
U6	Remote	Remote control of cooling and alarms.
U7	Apps	Other apps, e.g., for searching wine temperatures.
U8	Updates	Functional upgrades or security updates.

To obtain typical use cases for smart fridges, we have browsed the manuals and web pages of our selected devices. Table I lists all use cases we have identified. **Cooling** (U1) is the traditional use of a fridge. **Monitoring** (U2), **management** (U3), **shopping** (U4) and **remote control** (U6) refer to typical domestic requirements, which are now enhanced by digital services. Smartphone apps control cooling parameters and various alarms (opening, temperature, humidity), look inside the fridge via cameras, and might also identify food products that are used up or are close to its expiration date. If the smart fridge is part of a larger smart-home solution, it typically serves as a **multimedia** (U5) hub to deliver audio and video streams to connected devices. Some smart fridges allow **further apps** (U7), e.g., to manage recipes, to search for optimal wine temperatures or to browse the Internet. **Updates** (U8) are important to maintain the security and functionality of the smart fridge during its operational life.

B. IT Infrastructure Model

TABLE II. CATEGORIES OF DEVICES

Id	Name	Description
A1	Smart Fridge	The smart fridge.
A2	End-User Dev.	Smartphone (WLAN), TV, smart speaker, etc.
A3	Cloud	Digital fridge services on the Internet.
A4	3rd Party Serv.	Digital smart home services on the Internet.
A5	External Dev.	Smartphone (LTE) or tablet (LTE).

Table II lists all categories of devices or appliances needed to run the use-cases U1-U8. The **smart fridge** (A1) contains an embedded computing device with network interface and operating system. It may or may not also contain further plugins and apps, e.g. a web browser. Some smart fridges are equipped with internal cameras that monitor the stored food products. Any smart fridge we are aware makes use of sensors to monitor parameters, such as temperature and moisture. Both **end-user device** (A2) and **external device** (A5) are used to control any smart, digital service the fridge offers. Respective devices include laptops, smartphones, tablets, smart TVs or smart speakers. The difference between A2 and A5 is that the external device connects via LTE, i.e., it uses a network connection that leaves the home WLAN. Thus, we need to model it separately. A3 refers to a **cloud service** that is bundled with the smart fridge, and provides services tailored to the fridge. For example, Bosch KGN36HI32 connects to Bosch Home Connect. In contrast, A4 means any other **3rd-party service**, e.g., a smart-home system, a voice assistant or a content-delivery network from a third-party cloud. Since our focus is on the smart fridge, we leave aside the router.

TABLE III. CATEGORIES OF DATA

Id	Name	Description
D1	Sensor data	Video, audio, temperature, power consumption.
D2	App data	Data from apps installed on the smart fridge.
D3	Metadata	Timestamps, soft- and hardware versions.
D4	Configuration	Parameters, credentials, certificates.
D5	Telemetry	Device behavior, log information.
D6	Op. System	Software libs, updates, operating system data.

Use cases U1-U8 require the smart fridge to manage and share 6 categories of data with devices A1-A5, as shown in Table III. **Sensor data** (D1) includes any information delivered by internal sensors of the fridge, e.g., video streams from an internal camera or the temperature in the wine compartment. **App data** (D2) refers to data managed by the various kinds of apps executed on the smart fridge. Examples are the user's shopping lists, multimedia data from external parties or expiration dates. **Metadata** (D3) is any information produced by the operation of smart services. Examples include version numbers, timestamps or patch levels of software libraries. **Configuration** (D4) data stores parameters about how the use

cases should work. This means cooling parameters as well as WLAN credentials or HTTPS certificates. **Telemetry** (D5) means any information that is typically part of the log file of the smart fridge, e.g., internal errors, defrost times, power outage, and the like. **Operating System** (D6) refers to the program code of the operating system and its apps, updates, patches, libraries, etc.

TABLE IV. CATEGORIES OF ORGANIZATIONS

Id	Name	Description
O1	User	The user of the smart fridge.
O2	Vendor	The manufacturer of the smart fridge.
O3	Cloud Provider	The operator of the cloud service.
O4	3rd Party Provider	External cloud service providers.
O5	Other 3rd Parties	Other services.

The devices are operated by different parties, as shown in Table IV. Since our problem definition focuses on specific risks for a smart fridge, we leave aside the parties that might cause generic risks. Such parties are the Internet provider, the LTE provider or the electricity supplier. Large companies, such as LG, have their own cloud infrastructure and cloud services, like voice assistants used by the smart fridge. Thus, O2 and O3 can be the same organization.

TABLE V. CATEGORIES OF NETWORK CONNECTIONS

Id	Devices	Int.	Pers.	Description
C1	A1-A2	✓	✓	smart fridge – end-user device
C2	A2-A3	✗	✓	end-user device – cloud
C3	A1-A3	✗	✓	smart fridge – cloud
C4	A3-A4	✗	✓	cloud – 3rd party cloud
C5	A1-A5	✗	✓	smart fridge – external device

Table V contains all categories of network connections we need to consider. Note that all connections are bi-directional. Column "Int." indicates that a connection transfers data within the home WLAN. "Pers." means that a connection might transfer data related to the activities or habits of a person.

TABLE VI. ASSET MATRIX

U. C.	Data	Devices	Connections	Orga.
U1	D1, D3-D5	A1		O1
U2	D1-D4	A1, A2, A5	C1, C5	O1
U3	D2-D4	A1-A3, A5	C1-C3, C5	O1, O3
U4	D2-D4	A1, A2, A4, A5	C1, C4, C5	O1, O4
U5	D2-D4	A1-A5	C1-C5	O1, O4
U6	D1-D5	A1-A3, A5	C1-C3, C5	O1, O3
U7	D1-D5	A1-A5	C1-C5	O1, O3-O5
U8	D2-D6	A1, A3	C3	O2

After having defined the categories of use cases, devices, data, organizations and network connections we need to consider, we can define an asset matrix (cf. Table VI). The asset matrix tells which use case is tied to which IT asset. U1 (Cooling) is the only use case that does not need network connections, other devices or other organizations. All other use cases depend on an operational IT ecosystem.

C. Potential Harms and Damages

Table I allows us to devise four categories of potential harm, as shown in Table VII. The categories are in line with [20].

Potentially, a smart fridge may produce threatening physical or financial damages, e.g., from spoiled food or a violation of legal regulations. Negligible harm could be a brief interruption or malfunction of digital or cooling services.

TABLE VII. CATEGORIES OF POTENTIAL HARM

Category	Examples
negligible	Food spoils a bit earlier, digital services are unavailable for a short time, isolated false alarms.
limited	Fridge contents spoils, services are unavailable for some time, many false alarms.
substantial	Permanent unavailability of digital services or cooling results in a total economic loss, privacy issues.
threatening	High fines from violation of the law results in private insolvency, severe sickness from food poisoning.

From Table VII we can derive the protection needs of the data. In Table VIII, we have analyzed if an interruption, interception, modification or fabrication of data has an impact on integrity, availability or confidentiality. If this impact can produce negligible or limited harm, the protection need is normal. If it can be substantial, the protection need is high. If the harm can be threatening, the protection need is very high.

TABLE VIII. PROTECTION NEEDS

Data	Integrity	Availability	Confidentiality
D1	normal	normal	high
D2	normal	normal	high
D3	normal	normal	high
D4	high	high	high
D5	normal	normal	high
D6	high	high	high

D1–D5 might allow to infer personal information, e.g., eating habits, preferred foods, the daily routine or if the user is sick or on vacation. Thus, D1–D5 have "high" protection needs for confidentiality. The security of the user's network and the functionality of the fridge depend on D4 and D6. A misconfiguration, a disclosure of passwords, a manipulated OS update or an attacker knowing the patch-level of the software might result in a substantial harm (cf. Table VII). Thus, D4 and D6 have the protection need "high" for all three dimensions. In our domestic setting, a threatening harm is highly improbable, and we do not assign the protection need "very high". This may be different in other scenarios, e.g., if a hospital uses the smart fridge to cool medications.

The protection needs are inherited from the data to each IT asset managing the data, as listed in the asset matrix Table VI. The maximum principle requires that an asset is assigned with the highest protection need of all data it uses. For example, the vendor's cloud (A3) is part of the use case "Update" (U8), which includes data of the operation system (D6) with the protection need "high" for the protection dimensions integrity, availability and confidentiality. Thus, even if A3 handles less sensible data (D1 and D2), the protection need of A3 is "high" for each protection dimension.

From the asset matrix it follows that *any* device, network connection and organization need to maintain a "high" level of protection for each dimension, because either D4 or D6 is part of any use case. As consequence from the asset matrix,

TABLE IX. LONG-TERM COMPLIANCE RISKS

Risk	Orga.	Devices	Connections	Description
Privacy	O2-O5	A2-A5	C2-C5	Changing legislation, new codes of conduct, etc. impose limitations on the exchange of personal data with certain countries or parties [21].
Global Rules	O2-O5	A2-A4	C2-C4	New trade restrictions, sanctions, technology bans etc. restrict the use of an asset from certain countries or parties [22].
Local Rules	O1-O5	A1-A5	C1-C5	Local regulations, e.g., from environmental protection, consumer protection or electromagnetic compatibility, restrict the use of an asset [23].
Expiration	O2-O5	A1-A5	C1-C5	Disagreements to common compliance standards, expired certifications or approvals, non-renewed audits, etc., render the involved asset untrusted [24].
Concealment	O1-O5	A1-A5	C1-C5	Unknown characteristics at time of purchase disallow the further use of an asset, e.g., if it turns out that a build-in camera falls under espionage acts [5].

TABLE X. LONG-TERM ECONOMIC RISKS

Risk	Orga.	Devices	Connections	Description
Degradation	O2-O5	A3, A4	C2-C4	The service quality of an asset might be reduced, e.g., to nudge customers into new services by delaying updates or reducing performance of old services [25].
Licensing	O2-O5	A1, A3, A4	C2-C4	The revenue model might change. For example, an organization might switch its services to a pay-per-use model for an asset [26].
Discontinuation	O2-O5	A3, A4	C2-C5	One of the parties involved discontinues its service or makes it unattractive to use it from an economic point of view [27].
Liabilities	O2-O5	A3, A4	C2-C5	One of the parties involved discontinues its business, and its contractual liabilities become void at once [28].

TABLE XI. LONG-TERM OPERATIONAL RISKS

Risk	Orga.	Devices	Connections	Description
Inflexibility	O1-O5	A1-A5	C1-C5	Due to missing functional updates, it becomes challenging to connect an asset to recent services or devices [29].
Unreliability	O2-O5	A1-A5	C1-C5	The service level in terms of reliability, throughput, etc. of the asset degrades, e.g., due to reduced support for legacy products [30].
Unmaintainability	O2	A1	C1, C3, C5	Due to the use of outdated interfaces and closed-source components it becomes difficult to find manuals, experts or spare parts to that maintain the asset [31].
Insecurity	O2	A1	C1, C3, C5	Without security updates and by using out-of-date security protocols, the asset cannot be operated any more [30].
Defectiveness	O2	A1	C1, C3, C5	Modernizations in the IT ecosystem make technical debts of an asset visible, e.g., if a network protocol uses bits that were reserved for future use [32].

it is problematic to use a smart fridge as a multimedia hub in a smart home as well. Because the fridge runs services with "high" protection needs, the much less sensitive media-playback service must be secured at level "high" as well.

D. Long-Term Risks

After having identified the potential harms and the assets in our IT ecosystem that need special protection, we can compile IT-security risks. In order to obtain a comprehensive set of risks, we inspect each asset (organization, device, connection) in isolation, and we look for reasons why, at some point in the future, the asset in question will no longer operate as it did at the time of purchase. Recall that we are specifically interested in long-term risks of the smart fridge. Thus, in line with Step 3 of our research method, we filter out any potential risk that (a) is apparent at the time of purchase, or (b) is identical for a traditional fridge and a smart fridge. For example, we do not consider risks, such as the smart fridge is delivered with a pre-installed virus in its operating system, or the cooling unit fails after some time.

The resulting set of risks is long and repetitive, because some risks materialize across different assets. For example, licensing risks due to changing revenue models can affect many assets and network connections at some time in the future, and occur at multiple organizations. For this reason, we need Step 4 of our research method to consolidate risks.

Tables IX-XI show our consolidated set of long-term risks for 8 use cases for smart fridges. To our surprise, many of those risks are identical to the risks, which we had exemplarily identified for a single artefact (the network connection between a smart device and a cloud server) in [8]. This confirms the reproducibility of our research method.

We have structured our set of risks into three groups: **Long-term compliance risks** are produced by changing local, national or international rules and standards. Risks from this group mean that using the smart fridge may violate regulatory requirements in the future, even if it has fully complied with them at the time of purchase. **Long-term economic risks** are the result of future business decisions of the organizations involved. Seven of the identified use cases require a complex IT ecosystem, as shown in our asset matrix (Table VI). If an organization ceases operation or moves to a different revenue model in the future, the remaining IT ecosystem may no longer able to support all use cases in an economic manner. This also includes a pay-per-security-update model. Finally, **long-term operational risks** consider the technical perspective of operating a smart fridge together with its IT ecosystem for more than 10 years. Operational risks include technical challenges when trying to connect an outdated device to a

new one, and maintenance issues due to missing experts and spare parts for the IT ecosystem needed.

The tables only specify risks that impede a smart fridge, even if the same risk may be also associated with other devices in our IT ecosystem. For example, risk "Unmaintainability" is listed for device A1 (the fridge itself) and organization O2 (the fridge's vendor), although the same risk exists for any other IT asset that is used for a decade or more.

Note that even "cooling" (U1), the most basic use case, is at risk in the long run. A smart fridge may have a reduced control panel. Such fridges depend on the use case "remote" (U6), which needs an Internet connection to the vendor's cloud and a smartphone app. For example, the Samsung RF27T5501SG requires the user to download the "SmartThings" app and register for the Samsung cloud with a personalized account.

V. CONCLUSION

When non-smart devices are replaced by smart ones, the integrated IT components generate new risks, that may limit the operational life-span of the smart device unexpectedly. Such risks originate from different life cycles of digital and physical objects, from changing legislation, from future business decisions by the parties involved and from the technical complexity of the IT ecosystem needed.

In this paper, we have compiled a catalog of long-term risks for smart fridges. Our catalog consists of risks, which might materialize years after the purchase. The risks are specific to the smart device, i.e., we have omitted any traditional risk that also exists for conventional fridges. Because we have used a well-structured research method, we think that our risk catalog is exhaustive for compliance risks, economic risks and operational risks. Our risk catalog can be adapted to many use cases and smart devices that use a similar IT architecture.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[2] P. Zdankin, M. Waltereit, V. Matkovic, and T. Weis, "Towards Longevity of Smart Home Systems," in *International Conference on Pervasive Computing and Communications Workshops*, 2020, pp. 1–6.

[3] B. Schoon, "Android tv needs better standards for long-term updates and support," https://9to5google.com/2019/08/29/android-tv-long-term-updates-support/, 2019, retrieved: March, 2023.

[4] Frontier Nuvola Support, "Why did the service change on the 7th may 2019?" https://srsupport.frontier-nuvola.net/portal/en/kb/articles/service-change, 2019, retrieved: 2020-06-10.

[5] V. Gabrielle, "It sees you when you're sleeping: A clash of privacy and play," https://www.governing.com/security/it-sees-you-when-youre-sleeping-a-clash-of-privacy-and-play, 2022, retrieved: March, 2023.

[6] L. M. Tanczer, I. Steenmans, M. Elsden, J. Blackstock, and M. Carr, "Emerging risks in the iot ecosystem: Who's afraid of the big bad smart fridge?" in *Living in the Internet of Things: Cybersecurity of the IoT-2018*, 2018, pp. 1–9.

[7] Statista, "Average life expectancy of major household appliances in 2011 and 2022," https://www.statista.com/statistics/220020/average-life-expectancy-of-major-household-appliances, 2023, retrieved: March, 2023.

[8] E. Buchmann and A. Hartmann, "Identifying long-term risks of the internet of things," in *14th International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies (UBICOMM'20)*, 2020.

[9] A. Hevner and S. Chatterjee, "Design science research in information systems," in *Design research in information systems*. Springer, 2010, pp. 9–22.

[10] Bundesamt für Sicherheit in der Informationstechnik, "BSI Standard 200-3: Risk Analysis based on IT Grundschutz," *https://www.bsi.bund.de*, 2017, retrieved: March, 2023.

[11] 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.

[12] M. Aydos, Y. Vural, and A. Tekerek, "Assessing risks and threats with layered approach to internet of things security," *Measurement and Control*, vol. 52, no. 5-6, pp. 338–353, 2019.

[13] O. Garcia-Morchon, R. Rietman, S. Sharma, L. Tolhuizen, and J. L. Torre-Arce, "A comprehensive and lightweight security architecture to secure the IoT throughout the lifecycle of a device based on HIMMO," in *Symposium on Algorithms and Experiments for Wireless Sensor Networks*, 2015, pp. 112–128.

[14] J. L. Hernández-Ramos, J. B. Bernabé, and A. Skarmeta, "Army: architecture for a secure and privacy-aware lifecycle of smart objects in the internet of my things," *IEEE Communications Magazine*, vol. 54, no. 9, pp. 28–35, 2016.

[15] Digital Preservation Coalition, "Digital preservation handbook," https://www.dpconline.org/handbook, 2015, retrieved: March, 2023.

[16] S. Vermaaten, B. Lavoie, and P. Caplan, "Identifying threats to successful digital preservation: the spot model for risk assessment," *D-lib Magazine*, vol. 18, no. 9/10, pp. 1–21, 2012.

[17] H. M. Gladney, "Trustworthy 100-year digital objects: Evidence after every witness is dead," *ACM Transactions on Information Systems (TOIS)*, vol. 22, no. 3, pp. 406–436, 2004.

[18] G. Truman, "Web archiving environmental scan: Harvard library report," *Digital Access to Scholarship at Harvard*, 2016.

[19] J. Andersen, "Where games go to sleep: the game preservation crisis," https://www.gamedeveloper.com/business/where-games-go-to-sleep-the-game-preservation-crisis-part-1, 2011, retrieved: March, 2023.

[20] Bundesamt für Sicherheit in der Informationstechnik, "BSI-Standard 200-2, IT-Grundschutz Methodology," https://www.bsi.bund.de, 2017, retrieved: March, 2023.

[21] K. McCullagh, "Brexit: potential trade and data implications for digital and fintech industries," *International Data Privacy Law*, vol. 7, no. 1, p. 3, 2017.

[22] C. Ziye and L. Bin, "China-US High-Tech Competition, Trade Conflict and Development Rights," *China Economist*, vol. 15, no. 5, pp. 66–73, 2020.

[23] Council of the European Union, "Directive 2012/27/EU of the European Parliament and of the Council on energy efficiency, amending Directives 2009/125/EC and 2010/30/EU and repealing Directives 2004/8/EC and 2006/32/EC," Document 02012L0027-20210101, 2021.

[24] Y. T. Mak, S. Carr, and J. Needham, "Differences in strategy, quality management practices and performance reporting systems between ISO accredited and non-ISO accredited companies," *Management Accounting Research*, vol. 8, no. 4, pp. 383–403, 1996.

[25] D. A. Lyons, "Net neutrality and nondiscrimination norms in telecommunications," *Arizona Law Review*, vol. 54, p. 1029, 2013.

[26] M. A. Cusumano, "The changing software business: Moving from products to services," *Computer*, vol. 41, no. 1, pp. 20–27, 2008.

[27] M. A. Lemley and T. Simcoe, "How essential are standard-essential patents," *Cornell Law Review*, vol. 104, p. 607, 2018.

[28] A. Schwartz, "Products liability, corporate structure, and bankruptcy: toxic substances and the remote risk relationship," *Journal of Legal Studies*, vol. 14, no. 3, pp. 689–736, 1985.

[29] P. Mutchler, Y. Safaei, A. Doupé, and J. Mitchell, "Target fragmentation in android apps," in *IEEE Security and Privacy Workshops*. IEEE, 2016, pp. 204–213.

[30] B. Ford, "Icebergs in the clouds: the other risks of cloud computing," in *Hot Topics in Cloud Computing*, 2012, pp. 2–2.

[31] L. M. D. Ferreira, A. Arantes, and C. Silva, "Discontinued products," in *Conference on Operations Research and Enterprise Systems*, 2017, pp. 210–223.

[32] P. Kruchten, R. L. Nord, and I. Ozkaya, "Technical debt: From metaphor to theory and practice," *IEEE Software*, vol. 29, no. 6, pp. 18–21, 2012.