applied sciences

MDPI

Article

Towards a Maturity Model for IoT Adoption by B2C Companies

Olena Klisenko * and Estefanía Serral Asensio *

Research Centre for Information Systems Engineering (LIRIS), KU Leuven, Warmoesberg 26, 1000 Brussels, Belgium

* Correspondence: klisenko.olena@gmail.com (O.K.); estefania.serralasensio@kuleuven.be (E.S.A.)

Abstract: The fast-growing market for the adoption of IoT technologies poses serious challenges for companies providing IoT solutions. These challenges require constant technological and managerial improvement from the companies. To select the right direction for improvements, managers need appropriate tools for analysis and decision making. Recognised tools of this type are maturity models. Currently, maturity models developed for IoT adoption are mainly oriented to the business to business (B2B) market, while business to consumer (B2C) companies also need such a reliable tool for business improvement. Thus, this work is intended to fill the gap in existing research through the development of a maturity model for IoT adoption focused on the B2C market. To achieve this goal, we based our model on the scientific literature as well as on practical experience gained by leading companies in the market of IoT solutions. Moreover, the development and validation of the maturity model are carried out in close collaboration with two reputable European experts with extensive practical experience in this field. The result is a maturity model, which is a balanced, practice-oriented tool for assessing the maturity of the IoT solutions implementation and accounting for the specificity of the B2C market.

Keywords: Internet of Things; maturity models; capabilities; management of technological innovation

Citation: Klisenko, O.; Serral Asensio, E. Towards a Maturity Model for IoT Adoption by B2C Companies. *Appl. Sci.* **2022**, *12*, 982. https://doi.org/10.3390/app12030982

Academic Editor: Pedro Valderas

Received: 26 October 2021
Accepted: 21 December 2021
Published: 19 January 2022

1. Introduction

The Internet of Things (IoT) technologies have been present on the market for quite some time now and have already proven to bring massive benefits both for businesses and consumers. That is, IoT is used in smart manufacturing, logistics, energetics, healthcare, retail, home security and many more. Currently, the total number of interconnected objects amounts to 8.3 billion and is expected to increase to 21.5 billion by 2025 [1]. With the number of organisations adopting IoT products and services rapidly increasing, it is becoming easier to identify common difficulties they are facing in the adoption process. While information security and privacy are quite apparent points of concern, there are many more IoT-specific factors that need to be addressed for the implementation to be successful and actually generate value. For that matter, maturity models have been found to be effective for, firstly, the assessment and, secondly, the improvement in the process by breaking it down into highly detailed steps.

Although the topic of IoT is highly popular in the academic research community, surprisingly few studies focused on exploring it in the Business to Consumer (B2C) field. Most of the existing maturity and assessment models are either developed for the business to business (B2B) field or specify the dimensions and characteristics in a very general way, without considering the details that might be crucial for a B2C context. That being said, the aim of this research is to cover the described gap in currently existing studies by developing a maturity model specifically for the B2C context. Apart from contributing to the scientific knowledge pool of IoT, this paper also brings added value from the practical point of view. Organisations wishing to adopt IoT technology or to increase the efficiency of its current use can directly apply the developments of this research.

With this in mind, the research questions this thesis addresses are as follows:

R1: How can B2C organisations assess their current position in the IoT adoption process?
R2: How can B2C organisations achieve the next maturity level of IoT adoption?

This paper begins with a synthesised literature review (Section 2), that firstly introduces the IoT concept and then covers the topics of maturity models. Section 3 provides a discussion on the methods employed in the research to develop the IoT adoption maturity model. Then, Sections 4–6 present the analysis of three main sources of model dimensions identification. The process of the maturity model development, as well as the final model itself, are presented in Section 7. Finally, Section 8 provides a discussion on this research, including limitations and future research possibilities.

2. Literature Review: Maturity Models for IoT Implementation

Companies that are able to successfully implement IoT technologies extract added value and gain a competitive advantage. However, due to the still emergent nature of IoT, no specific procedures and standards have been defined yet regarding its implementation, which is the root of many adoption-related issues and challenges. IoT service providers tend to employ a "learning by doing" strategy, which obviously does not generate expected added value and does not justify the cost of the IoT implementation [2].

Maturity models are said to be a powerful tool for organisations to use in order to achieve their strategic objectives. It assists in understanding the current state of effectiveness, identifying the need for change, and deriving the steps that have to be taken to improve the current position. As stated in a study by Klötzer and Pflaum [3], maturity models can be classified as staged, continuous, or focus area oriented. With regards to their purpose, Klötzer and Pflaum [3] also distinguish descriptive, prescriptive, and competitive types of models.

The most well-known maturity model in the IT field is the Capability Maturity Model (CMM). Originally proposed by Paulk, Curtis, Chrissis and Weber [4] to assist the process of software development, specifically in government projects, the CMM later evolved as a tool for improving business processes in general. The model consists of five levels of maturity and moving along them constitutes enhanced effectiveness in the use of a product or service.

Since the CMM proposal, many other maturity models were proposed. Table 1 provides an overview of the models created for maturity assessment in areas of innovation development and implementation on the basis of information technology, primarily IoT, as well as in the areas of data management and analytics.

After analysing the IoT maturity models, it becomes clear that there is no consensus about the crucial pillars of IoT implementation maturity. Different capabilities are prioritised in these models, with the exception of technology, data and organisational culture, which are, however, still included in the models under different structural compositions and varying definitions.

No maturity model for IoT was found to be specifically designed for the B2C market and be reflective of the factors important for operating under its conditions. In addition, although a large range of various maturity models has been developed, their usability and actual effectiveness are arguable. Felch, Asdecker, and Sucky [20] claim that particularly scientific maturity models in practice fail to meet users' requirements. This drawback is due to the lack of customizability and adaptability of such models. The findings show that organisations prefer to either develop their own maturity models specifically tailored to their internal goals and needs or make use of the models proposed by consulting firms, which heavily rely on industry experts' opinions and experiences in the development of the model. For this reason, it is important to continue the development efforts for IoT maturity models, focusing on the one hand on having a strong basis of academic knowledge, and on the other hand on reflecting the best practices and real solutions of the companies implementing IoT technology in their businesses.

Table 1. Reviewed maturity models.

Name	Purpose	Model Specification	Reference
Three stages maturity model in SME's towards industry 4.0	Digitalisation of SME	5 maturity stages, 3 dimensions	[5]
Industry 4.0-maturity model	Industry 4.0	6 stages, 5 dimensions	[6]
The IoT technological maturity model	IoT implementation for manufacturing enterprise	8 maturity stages, 1 dimension	[7]
Supply chain systems maturing towards the internet of things (IoT)	Information and communication technology deployment	4 stages, 4 dimensions	[8]
Maturity model for digitalisation	Digitalisation	5 stages and 9 dimensions on two facilitators of digital transformation	[3]
System integration maturity model industry 4.0	Evaluation of I4.0 IT capabilities	5 stages, 4 dimensions	[9]
Industry 4.0 maturity model	Industry 4.0	5 maturity stages, 9 dimensions	[10]
Maturity model for data-driven manufacturing	Analysis of IT architecture	5 stages, 1 dimension	[11]
Maturity Levels for cyber-physical systems	Building CPS capabilities	2 layers, 5 stages on each, 1 dimension	[12]
IoT solutions maturity model	IoT implementation	34 parameters classified in 9 groups	[13]
Integrated IoT capability maturity model	IoT implementation	5 stages, 3 dimensions;	[14]
IoT security model	IoT security implementation	3 domains, 5 comprehensiveness levels, 3 scope levels	[15])
Gartner's IoT maturity assessment	Identifying organisation's IoT readiness	3 maturity levels, 2 dimensions	[16]
TDWI readiness model for IoT	Identifying organisation's IoT readiness	Level of readiness assessed on the score out of 20, 5 dimensions	[17]
Axeda's connected product maturity model	IoT implementation for production companies	6 maturity levels, 1 dimension	[18]
Maturity model for IoT in retail industry	IoT implementation	5 maturity levels, 5 dimensions	[19]

3. Research Methodology

To create the maturity model for IoT adoption in the field of B2C, we have followed a top-down approach as proposed by Becker [21]. As such, we identified first the dimension and levels of the model, and then we identified the sub-dimensions across the maturity levels.

To collect the necessary data for creating the model, three sources of information were consulted: literature (Section 4), expert opinions (Section 5), and successful case studies (Section 6). The conclusions drawn from the analysis of these sources were considered to have an equivalent level of importance for the identification of the model dimensions and sub-dimensions.

To begin with, a thorough literature review was conducted to, firstly, obtain an understanding regarding the already existing maturity models for IoT, and, secondly, to identify essential points and most common challenges that organisations face when implementing IoT technologies. The results of this analysis were used for two purposes—(a) creating and structuring interview questions and (b) identification of the model dimensions. In order to locate papers for the literature study, Google Scholar was utilised. The following keywords were used: *IoT maturity model*, *IoT adoption*, *IoT implementation*, *IoT adoption challenges*, *IoT adoption factors*, and *IoT adoption in B2C market*.

The next step in this research was the set-up of and preparation for the first in-depth semi-structured interviews with the companies operating in IoT. Obtaining input from the industry experts to use for the development of the model was crucial for ensuring that the model is practically valuable and can be effectively used by organisations. To avoid bias, the maturity model was not constructed prior to the interviews, and the interview questions were developed to be broad in nature. Such design encouraged experts to actually give their personal opinion instead of just their evaluation of an already existing model. Two experts were interviewed, both occupy high positions in their organisations and have more than 20 years of working experience in IoT and innovations. The experts were also familiar with the concept of maturity models and their structure.

Afterwards, three IoT adoption cases were reviewed to identify dimensions and sub-dimensions of the maturity model. The study of implementation cases allows forming a clear understanding of the challenges companies adopting IoT solutions face, both from the point of their internal readiness and from the point of market forces, i.e., consumers, suppliers, and rivals. Moreover, the study of cases allows reviewing the decisions compa-

nies made to tackle those issues. This analysis served as a solid foundation for practical-oriented structuring of the model and dimensions identification.

After the processing of the data from the first interviews and the analysis of the literature and cases were finished, the initial version of the model was developed. In order to evaluate and further refine this model, it was sent to the experts who were asked to review the identified dimensions and sub-dimensions. Specifically, the experts were asked whether they agreed with the model dimensions and sub-dimensions or considered that they needed to be removed, combined, or if other (sub-)dimensions needed to be added. This information was then discussed during a follow-up interview and the structure of the model was refined and finalised taking into account this feedback. Afterwards, the definitions of dimensions, sub-dimensions, and maturity definitions across the maturity levels were completed and validated once more with the experts. The answers of the experts were noted (see Supplementary Materials S2 and S3), and all the interviews were tape-recorded.

4. Identified Dimensions from the Literature Analysis

This section discusses the dimensions identified from the analysis of the literature on the topic of implementing IoT solutions. The selected dimensions are satisfying one of the following criteria:

- They are the most frequently mentioned in the maturity models for IoT adoption and are regarded as important pre-conditions to the realisation of an IoT project of a company. These dimensions are:
  - Technology—[7,8,13,14,16,17,19].
  - Data (management and analysis)—[8,13,14,17,19].
  - Organisational culture (also defined as authority and culture)—[8,14,17,19].
- They are frequently mentioned as adoption challenges or aspects to be considered in the adoption process. These dimensions are:
  - Security and privacy—[22–24].
  - Data management and analysis—[25–30].
  - Communication with consumers—[31–33].
- They are practice-oriented recommendations for IoT project implementation. The following dimension belongs to this category:
  - Strategy—[34–36].

4.1. Technology

Unsurprisingly, the first factor driving the process of IoT integration is technology. The presence of necessary software and hardware, i.e., infrastructure, enables the use of IoT in a company.

To understand what kind of technology is needed for IoT integration, it is important to first understand the structure of an IoT system. As explained in the article by Maliping [37], an IoT system consists of five layers: perception, access, network, management, and, finally, application. Firstly, at the level of perception, various data is being collected and transformed into signals to send to the devices. Secondly at the access and network level, collected information is transmitted to and integrated into the network through already present networks, such as mobile communication, satellite, and local networks. Next, the service management layer is responsible for monitoring existing networks and making sure that processes on other levels are flowing smoothly. Finally, application level is the level of the IoT system where collected information is being analysed, and the appropriate response is generated to be sent back to devices. According to the author, examples of this process are real-time health monitoring, intelligent power grid, etc.

To enable the aforementioned essential processes, different kinds of technologies are required. Four types can be distinguished: device hardware, device software, communications, and platform (What Technologies are Used in IoT-Technology Behind Internet of Things. (11 June 2019). Retrieved from https://www.avsystem.com/blog/iot-technology/

(accessed on 16 December 2019). Necessary device hardware, such as sensors and actuators, as well as computing hardware are needed for processes at the Perception level to be realised. Likewise, device software enables all operations performed by smart devices. They include data collection and its real-time analysis, sending and receiving information from the Cloud, and managing devices. Next is communication technology, which supports processes on all levels of an IoT system. As stated by Maliping [37], "*Communication technology is a key technical measure for connection and communication among things in the Internet of things, playing an irreplaceable role in development of IoT.*" Here, apart from the installations of the necessary hardware, data transfer protocols must also be considered. Choosing an appropriate one to support the interaction of devices with the Cloud and among themselves is important for the whole functioning of the IoT system. The working range of the communication solution varies, so the choice should be made according to the needs of a particular system. Last but not least, is the platform. It is a collective of software and hardware that constitutes the core of the IoT system. Collected data is being processed at the Cloud or on-site server, and the decision regarding the next actions within the system is made. Bandyopadhyay and Sen [27] also discuss that, when authorising actions to be performed by devices, the decision-making algorithms need to consider multiple sensor observations and relationships among them instead of only one.

It can be seen that there is a lot to consider in the aspect of technology. IoT Project Management [38] as well emphasises that there are a plethora of decisions involved when working through these aspects of IoT adoption, so the matter of technology should be considered thoroughly.

4.2. Data Management

Companies employing IoT technology are dealing with huge amounts of data. However, simply collecting this data does not bring real value to the company. Actual benefits can only be extracted from the results of the analysis of the data and the consecutive decisions based on it. As explained by Lee and Lee [25], these data are used for the identification and finding solutions to business issues, such as changing customer behaviour and market conditions with the aim of increasing customer satisfaction, etc. Vice president and analyst at Gartner, Ted Friedman [26], stated that one-third of IoT solutions will be abandoned before deployment due to the insufficiency of data management and analytics capabilities adapted for IoT.

The issue of data management is frequently mentioned in the literature on IoT implementation as a challenge, or adoption barrier. That is, Bandyopadhyay and Sen [27] state that in order to provide valuable services, management of large amounts of data is necessary. Singh and Singh [28] argue that, while every 'thing' in the IoT environment is able to generate huge amounts of information, the actual challenge of IoT adoption is the storage, security, and analysis of collected data. The same argument is again supported by Evans [29]. Moreover, Kamble et al. [30] discuss that in light of rapidly growing IoT networks and consequent scalability issues, companies have to be ready to face the challenges of data collection, storage, processing, analysis, and service provision.

4.3. Organisational Culture

Organisational culture is mentioned frequently in existing maturity models for IoT. According to Vachterytė [14], the culture of a company is a vastly important factor for improving IoT implementation. Plainly implementing IoT technology will not bring a company any real value until the corporate culture is adapted to new digital technologies [39]. Employees of the company going through the adoption process of new digital systems need to learn to trust these systems and accept their suggestions. The authors further explain that there are two main enablers of cultural change—willingness to change and social collaboration. The former refers to the willingness to detect changes in the environment and adapt to them. It is important that individuals working in the company learn to recognise opportunities for change in their environment and initiate subsequent actions to obtain the

value out of them. The same is supported by Büyüközkan and Göçer [40]. The resistance to change will divide the organisation into those adapting to the new technology and those trying to work employing the old familiar methods, which causes the delay in the adoption.

The latter term, social collaboration, encompasses the openness and trust in the organisational culture, which enables the unrestricted exchange of knowledge among employees. It is important to emphasise the data-driven decision making emerging from the above-described cultural change facilitators [39]. Data should be the basis for decisions in the company, rather than the personal judgements of individuals. Employees need to gain confidence in the data and be able to learn from it to build an entire decision-making process around continuously collected data.

What is more, IoT adoption is explained in the IoT Project Management [38] as a multidisciplinary process, which requires the involvement of people from various departments of the organisation. They include financial, R&D, sales and marketing, IT, human resources, and operations departments. From this, it is possible to conclude that the team working on the IoT implementation project should include experts from all mentioned departments.

4.4. Communication with Consumers

Another important perspective to consider while investigating IoT adoption concerns the viewpoint of consumers. Here consumers are understood as end-users, who use and interact with IoT solutions. Al-Momani, Mahmoud, and Sharifuddin [31] found that the most important variables figuring in the implementation process apart from already discussed information privacy and security concerns are perceived usefulness, perceived ease of use, trust, and cost. While the last factor is straightforward for understanding from the point of view of the consumer, the others require a more thorough analysis.

Although formulated slightly differently, the term perceived usefulness is present in several models (i.e., technology acceptance model, unified theory of acceptance and use of technology, diffusion of innovation) and explains a single concept in all of them—the added value to the performance users of the new technology expect to obtain from adopting it [31]. Gao and Bai [32] found that the consumers' perception of usefulness is the most significant predictor compared to other mentioned variables. Equivalently, AlHogail [33] reports that the level of satisfaction with the actual IoT product compared to the expectations is said to have an impact on consumer's trust, which in turn affects the willingness to adopt that product. This finding was also backed up by an empirical study in the same research, where perceived usefulness received the highest number of responses indicating it as a favourable factor for the IoT technology adoption. Having said that, it is sufficient to conclude that developers of IoT products and services need to ensure that the usefulness of their offer is clearly communicated to the end users.

Similar to the previously discussed concept, perceived ease of use has also received a lot of support as a factor greatly influencing the IoT adoption process [32,41,42]. Davis [43], defines it as "*the extent to which a person believes that using a system would be free of effort*". That being said, IoT product developers should ensure that consumers find it easy enough to adopt and use. However, as stated by Jalali et al. [23] it is crucial to keep the balance between the design simplicity of the product for customer attraction and the strength of cybersecurity for reducing the probability of hacking attacks.

Trust is proved to be another significant factor in the IoT adoption process, as it is precisely what offers consumers the incentive to use an IoT product even considering all the risk and uncertainty involved [33]. The author further stresses the need to include trust in the adoption models with the aim of gaining insights on the aspects influencing consumers' willingness to adopt an IoT product or service. For consumers to develop and retain trust in the product, IoT providers must ensure strong data protection and a high level of product functionality. The aforementioned factors, i.e., perceived usefulness and perceived ease of use, apart from being independent influencers of the IoT adoption process, also appear to have an impact on the level of consumer trust from the product-related dimension. Social

dimension variables, such as consumer networks were also found to affect consumer trust, however, not to the same degree as security- and product-related factors.

4.5. Security and Privacy

The most frequently mentioned and thoroughly discussed issue is information security and privacy. Microsoft reports that 97% of companies adopting IoT are worried about the question of security [22]. IoT providers are focused on developing and introducing enhanced product functions and interconnectivity, while poorly regarding the concerns of cyber security and protection of consumers' data [33]. Jalali, Kaiser, Siegel, Madnick [23] state that users' both real and perceived fear of cyber risk is one of the most serious obstacles to market adoption of IoT products and services. IoT devices are able to autonomously collect various data and transfer it to the Internet, enabling live analytics in this manner. Data collected from users might include information about an individual's health, their shopping preferences and history, location, financial data and etc. [28]. Undoubtedly, potential users are deeply concerned with the possibility of such information being leaked or stolen, which negatively impacts their willingness to make use of IoT technology. Hsu and Lin [24] distinguish four categories of privacy concerns in an IoT context: collection, unauthorised secondary use, improper access, and errors.

Jalali et al. [23] discuss the concept of perceived cyber-security risk and propose an Iceberg model to break down the flow of the IoT products development, deployment, and improvement taking into account the question of cyber security. The visible part of the iceberg above the water surface represents the way market adoption benefits product development, but for the sake of addressing the question of the impact of cybersecurity on the IoT product attractiveness, the focus here is on the bottom part of the model, i.e., part of the iceberg hidden under the water. The authors argue that the unwillingness to adopt a certain product might be caused by some factors located "below the surface". That is, the growth of the market size leads to hackers becoming more attracted to the product, which in turn increases the probability of cyberattacks being successful. Cyber-risk exposure is one of the components of users' perception of security and reliability, so it significantly affects how beneficial they think IoT product is. If the perceived risk outweighs perceived benefits potential customers will choose not to adopt the product.

The authors further discuss that organisations face a choice when dealing with the issue of perceived cyber risk. It boils down to two options: either starting to invest in developing cybersecurity capabilities right from the design stage of IoT product development, or acquiring them when the product is already on the market and the company has been receiving stable revenues. Findings in this study show that organisations investing in cybersecurity from the very beginning are less likely to be attacked by hackers and also enjoy a higher level of perceived reliability from the consumers' side. However, this option might not be available for start-ups, which only control limited financial, human and time resources.

To tackle the issue of information privacy and protection, Leonard (2017) stresses that IoT providers must clearly communicate the terms and conditions of the use of their products and services to the consumers so that the use of their information is clearly understood. Moreover, Anciaux [38] explains that risks related to the IoT adoption have to be identified together with their livelihoods, the potential impact must be determined, and based on that, measures to reduce the risk and impact must be developed. In addition, Hsu and Lin [24] summarise three types of guarantees that should be offered to end users: awareness of the privacy risks related to the use of IoT products, individual control over the collection and processing of personal information by smart objects; and awareness and control of subsequent use of personal information by external parties.

Furthermore, organisations implementing IoT may want to consider making use of The National Institute of Standards and Technology (NIST) cybersecurity framework. Jalali et al. [23] claim that NIST is currently the leading framework. Moreover, Shackelford et al. [44] view NIST as a tool that potentially can become the international standard of cybersecurity. Originally,

this framework was developed to protect critical infrastructure units, such as banking, from cyberattacks, but it appeared to be applicable for many other cases. Due to its general and non-specific application to certain technology structures, the NIST cybersecurity framework can be used by organisations of any size and facing different levels of cybersecurity risks [45].

4.6. Strategy

Another area crucial to be transformed or developed for successful IoT adoption in a company is *strategy*. For instance, Kranz [34], in his practically oriented book on IoT projects implementation, dedicates a section to the discussion of the Vision and Path stage of an IoT project. The contents of this section have a clear relation to the question of the strategy of a company integrating IoT. Moreover, the author introduces a number of strategic tools to thoroughly plan IoT integration efforts, such as business use case definition, IoT business case value proposition development, benchmark analysis, and ROI analysis. Therefore, refinement of the organisational strategy and its alignment with the use of IoT technology is an important part of the adoption process.

Caro and Sadr [35] in their extensive study on the IoT strategy development, proposed a framework to assist with the formulation of the said strategy. The framework distinguishes IoT opportunities according to their associated capabilities and the value they create. The two types of capabilities are enabling and enhancing capabilities. The former generates value for the company by making existing processes more efficient, while the latter creates unique opportunities that are otherwise not possible to realize. Enabling opportunities are typically easier to identify, as they directly relate to the company's operations.

A company's capabilities and its significance for formulating an IoT implementation strategy are also discussed by Slama, Puhlmann, Morrish, and Bhatnagar [36] in their book on enterprise IoT. Jim Heppelmann and Prof. Porter, in their article on connected products, as summarised by Slama et al. [36], presented a framework of 10 strategic questions to tackle in the development of a company-specific IoT strategy. The questions fall under one of the four major categories: Product and service, technology, data, and business strategy. The process of strategy definition flows sequentially through these four categories, starting with the identification of the capabilities to pursue, technology-related considerations, clear understanding of which data to collect, how to manage data ownership and monetization. Finally, a number of questions concern the business strategy, particularly, possible changes to the business model and the scope of business operations. This actively demonstrates the significance of strategy formulation for IoT adoption.

5. Case Studies Analysis

Among the many practical examples of implementing IoT solutions, three cases were selected for consideration in this research:

- Port of Hamburg, where IoT is an integral part of the smart transformation of the port;
- IoT implementation in the leading heavy equipment company;
- IoT implementation in retail.

The choice of these cases is due to the fact that their analysis, firstly, made it possible to obtain a holistic view of the practical approach of leading companies to the implementation of IoT solutions, and, secondly, provided grounds for creating working hypotheses regarding key dimensions of the studied maturity model.

5.1. Port of Hamburg

The first IoT adoption case reviewed is the case of the Port of Hamburg written by Sia Partners [46]. It is one of the biggest ports in Europe and a pioneer in the integration of IoT technologies. Technological innovation is highly important for Hamburg's Port to continue business growth and remain competitive on the international scene. By 2025, the management of the port are aiming to transform it into a smart port, as written in the 2025 Port Development Plan. It is clear from the presence of such an extensive document

that the integration of IoT technology has a strong strategic foundation in it. Therefore, a dimension *strategy* was identified. A smart port encompasses three pillars: smart port infrastructure, intelligent traffic flows, and intelligent trade flows. The IoT technologies adopted to empower the smart transformation in the area of smart port infrastructure include smart lighting, smart storage systems, smart maintenance sensors monitoring the use of assets and infrastructure, as well as sensors for security purposes. Moreover, IoT is also used to make Hamburg a green port. That is, sensors monitoring such parameters as temperature and pressure are installed to control the energy use in the port. As for the intelligent traffic flows, the use of IoT is seen in the installation of sensors monitoring the traffic and parking in the port. In the area of intelligent trade flows, IoT technologies allow the port's management to track every good moving around the port, efficiently manage deliveries, and reduce labour costs by reducing the number of physical checks needed at customs control.

Further reviewing the case study, it became clear which difficulties were faced by the port's management in the process of IoT integration. The challenges indicated in the case study are: heterogeneous technologies, fear of transparency, and business process reengineering (BPR). The first one relates to the issue of integrating different technologies together to create a smart network. There is a strong need for the development of common technological and transmission standards in order to ensure that connected devices can freely communicate in the same language and efficient data management can be achieved. Moreover, a modular approach is advised to be followed, such that new system modules can be easily added to the existing system. This takeaway makes it clear that *technology* is of course a vital part of IoT implementation and must be included as a model dimension. Moreover, the question of *standardisation* of technology and communication appears to be important as well, therefore, it is included in the model as a sub-dimension under dimension technology. The same is observed in the IoT Project Workbook.

The second challenge is fear of transparency. It concerns data privacy and security within the IoT network. Free transmission of data over the IoT network is an integral part of IoT technology. Naturally, with many parties involved, there is a big concern about the safety of information being disclosed. In the case of Hamburg Port, many firms doing business with the port were reluctant to share their information with the central management that processes it. Because of this, many resources were put into building a secure data management system and communicating with the said companies to ensure them about the safety of the data they share. From this follows the identification of *data security and privacy* sub-dimension(s) under the dimension of data. The inclusion of these sub-dimension(s) is also supported by the literature analysis and the views of both experts.

The final challenge highlighted in the case study is BRP. Here, the central message is that simply adopting IoT technology is not enough—efforts aimed at reengineering the related business processes are needed. As many stakeholders are involved in this process, BRP requires a thorough approach and takes a lot of time in order for the result to be successful. Thus, the *business processes* dimension is identified.

Next-discussed are the best IoT adoption practices that can be learned from the case of Hamburg Port. To begin with, an inclusive stakeholder approach is presented as one of the essentials to IoT system development. The requirements of those to be involved in the IoT system need to be taken into account right from the start of the implementation process. The fundamental of IoT integration is the identification of the business needs that IoT technology will tackle, followed by the planning of the necessary changes in business processes and analysis of technology that would be required. Here, once again, it is clear that business processes and technology need to be included in the model. The next helpful practice is the involvement of cross-functional teams in the process of IoT integration. Because of the many areas that need to be considered when adopting IoT, having a team of people who can provide a complete view is highly valuable. The sub-dimension *IoT team* is identified and included in the model. A strong partnership structure should be built with parties able to support different integration aspects. Therefore, it is possible to identify

dimension *communication with partners*. In addition, as mentioned previously, a modular approach should be taken from the start of the integration to allow for the transformation process to flow on a project basis and eventually result in a fully integrated IoT system.

5.2. IoT in a Heavy Equipment Company

In this case study Cognizant [47] makes a walkthrough of their IoT solution designed for and implemented in a leading heavy equipment company. It is described in the report that originally the company in question has been collecting enormous amounts of data to power equipment and fleet management. However, this effort did not bring expected added value, because still all strategic business units involved were isolated from one another, and, as a result, solutions they developed were not aligned. From this situation, it is possible to learn that collecting big amounts of data alone does not bring any real value to the company. It only comes once the company starts to properly utilise and deduct insights from this collected data. The same argument was already mentioned in the interview with Expert 1. Therefore, the dimension *data* with the sub-dimension *data management* is identified, reinforcing the same conclusion from the analysis of both expert views and literature analysis.

Furthermore, Cognizant explains in this case study that in order to enable this IoT initiative, a unified platform for storing, managing, and analysing data collected by sensors installed on the equipment was implemented. This platform allows managing data from all strategic business units, solving the issue with their solutions not being aligned. From this, it is clear that the *technology* dimension can be identified, because the IoT platform, as explained in Section 4.1, is an integral part of IoT infrastructure. The significance of technology is also emphasised in the Hamburg Port Case.

5.3. IoT in Retail

Another case study by Cognizant [48] begins with describing the challenge a grocery retailer in question was facing—high food waste and energy costs caused by inefficient management of food refrigerators and overall temperature in stores. Quite a lot of time is spent on the detailed definition of the business problem and how IoT can solve it. From this a clear connection can be established to what was learned from the IoT Project Workbook and Hamburg Port Case—any IoT initiative should have a solid business foundation. This argument was mentioned in the expert interviews as well. It can also be concluded that with the implementation of IoT technology in this company some rethinking of business processes took place, particularly in regard to store management. Therefore, it is possible to identify the *business processes* dimension.

To solve the described business problem Cognizant integrated an IoT platform that allowed to optimise the management of already installed temperature sensors. As a result, in most cases the temperature in stores became self-regulating thanks to the algorithmic decision making, decreasing the number of times a technician has to be called to adjust it. The installed system is also able to perform preventive analytics and predict failures. Of course, the implementation of such a solution would not have been possible without technology and the setup of the required infrastructure. Thus, the dimension of *technology* is identified. It is also in line with the conclusions deduced from the literature and Hamburg Port Case.

6. Expert Views

The analysis of the first round of expert interviews revealed the following conclusions regarding the maturity model dimensions.

6.1. Expert 1 Interview

When asked about the most important in the IoT products, the expert built his response around the significance of using data collected by the IoT devices to make better and faster decisions. Even more, this message is traceable throughout the whole interview—IoT is

not about smart things, but about data and understanding how it can be used to the benefit of the people. From this, it is quite obvious that *data* is the central concept in IoT and it definitely should be one of the dimensions of the model. Moreover, since the real value of IoT comes not from merely collecting data, but from effectively using it to improve decision making, a *data management* sub-dimension should be included in the model as well to define the collection, management, and use of the data. In addition, because of the fact that the major benefit of using IoT is making better decisions, it is possible to track the maturity of IoT adoption in the company through the way IoT is integrated into its decision-making process. Consequently, the *decision-making* sub-dimension should be added to the model.

Further on, the expert explained the opposite side of the benefits brought by collecting data—the risk of it being stolen and used in fraudulent interests. The issue of data security needs to be addressed by all parties involved. That is, product developers need to make sure they are employing up-to-date security measures, while the users should have the latest software updates installed and change their passwords regularly. Closely tied to security is the issue of information privacy. However, the expert emphasised that it is more of a legal matter than a technological one. It is the law that defines what privacy is and what companies need to abide by. Having said that, it is possible to identify *data security and privacy* sub-dimension(s) under the dimension of data. Whether data security and data privacy should be included as separate or as one sub-dimension was put under discussion with the experts in the second series of interviews.

What is more, organisational *strategy* sub-dimension under the *organisation* dimension was identified from the interview. The expert explicitly stated that the integration of IoT in the organisation needs to be fully aligned with its strategy.

Interesting is the discussion of the expert on the transition of IoT products from being sold as a product to being sold as a service. This is due to the fact that after the product is sold to the client, it does not end there. Data from the IoT devices are being continuously collected and interpreted, and the continuity of this process is what transforms the IoT into a service model. A possible (sub-)dimension that can be identified is therefore *business models.*

6.2. Expert 2 Interview

The takeaways from the interview with the second expert are in many points similar to those of the first one. First of all, according to the expert, the value of IoT technology lies in it unlocking new benefits. For different parties using IoT these benefits can constitute different things—for companies it might be lower cost, and for normal people, it may unlock new ways of shopping. In general, it boils down to doing things in an easier, quicker, cheaper, more integrated, or faster way. The same is applicable to the decision-making process in organisations—it becomes simpler, faster, and less hierarchical. Here it is possible to draw a connection to the interview with the first expert, who also mentioned simplification and improvement in the decision-making process. Likewise, the *decision making* dimension can be identified.

Secondly, the question of security and privacy was once again regarded very seriously. The expert mentioned it as a major issue related to using IoT, because there are people who might steal the collected data. Thus, a *data security* sub-dimension is identified to be included in the model under dimension data.

Furthermore, the expert explains that IoT needs to be fully integrated into the organisation for it to bring real value, it is not enough to simply install the technology. The appropriate changes need to take place at the level of products, processes, and people. Considerations regarding how to make the product offering competitive and valuable in the digital world are inevitable. It is, therefore, safe to conclude that IoT integration needs to be aligned with the *strategy* of the organisation, and such a model sub-dimension can be identified. Next, IoT adoption is tied to the processes in the organisation. Finding solutions for their optimisation under IoT technologies and overall digitalisation is a major task. Therefore, the *business process* dimension should be included in the model to account for this. Additionally, different stakeholders are involved in the IoT adoption process. On the

one hand, it is important to consider the users of technology and their characteristics, such as age and culture, which have an impact on their interaction with IoT. For example, people in their 20th interact with technology way more intuitively than people in their 50th and this has to be taken into account. So-called by the expert non-digital people, need to be kept on board with the happening digitalisation and provided sufficient information to understand what it is about, how it works, and what benefits it brings. On the other hand, people in organisations adopting IoT technology also have to be regarded, as they need to possess the necessary knowledge in order to understand and correctly work with this technology. The dimensions *communication with customers* and *organisational culture* can therefore be identified.

7. Maturity Model

This section contains the results of the maturity model development. The first subsection presents the initial maturity model. The second subsection describes the process of maturity model evaluation via experts' opinions and literature support. The final version of the maturity model after its refinement and completion is presented afterwards.

7.1. Initial Maturity Model

Figure 1 presents the overview of the identified dimensions and sub-dimensions of the initial model. The identified (sub-)dimension is linked to the applicable main data source(s)—literature (L), expert interviews (E), and/or case studies (CS). The references to specific section(s) in the paper containing the basis for the identification of a particular (sub-)dimension are presented in Supplementary Materials S4.

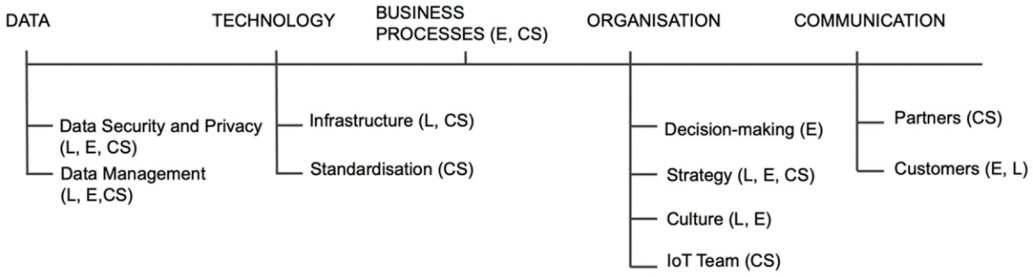

Figure 1. Initial model.

As for the maturity levels, the choice was made based on the literature and existing models. It was observed that in most cases there are five maturity levels (see Table 1), so for the present model, it was decided to stick to five levels as well. They maturity levels definitions of the COBIT (control objectives for information and related technologies) framework developed ISACA [49] were applied with modifications:

Level 0: Non-existent—the process is not existent at all.

Level 1: Initial/ad hoc—no standardised processes are in place.

Level 2: Repeatable but intuitive—procedures are followed but there is still a high degree of reliance on the knowledge of individuals.

Level 3: Managed and measurable—procedures are standardised and consistent, significant errors are detected and prevented. Documentation is complete and the compliance with required procedures is measured.

Level 4: Optimal and robust—a refinement of processes to a good level of practice took place and variances are constantly reduced. The system is benchmarked against the best-in-class standards and practices.

It is important to clarify the structure of a number of dimensions in the initial model. Technology dimension includes sub-dimensions infrastructure and standardisation. Although standardisation was originally identified as a separate dimension, it was decided to include it under the technology dimension, because it is a closely related concept, understood as the standardisation of technology. It only makes sense that it exists

as a sub-dimension to further serve the explanation of maturity evolution in technology. Next, decision making, strategy, culture, and IoT team, which were originally identified as separate dimensions, were grouped under dimension organisation, as they all explain changes necessary to be made in the management aspects of the organisation. Finally, communication with customers and communication with partners were originally identified separately, and later logically grouped under one dimension—communication.

7.2. Maturity Model Refinement and Validation

A second series of interviews was conducted to evaluate the initial model and the structure of dimensions and sub-dimensions was refined accordingly. After collecting the feedback from the experts, the changes they proposed were implemented as long as they were supported by any of the other two main sources of information (i.e., literature or adoption cases).

In general, the initial maturity model received positive feedback from the experts. The choice of five maturity levels was approved, with minor modifications to their definitions. Both of the experts also approved identified dimensions and sub-dimensions.

Both experts stressed the importance of adding a Data Analytics sub-dimension to the dimension Data. It was argued that the dimension *Data Management* does not include the processes related to processing, analysing, and extracting the value from data, which is one of the main purposes of IoT. Therefore, the sub-dimension *Data Analytics* was added. Next, both experts also pointed out that the initial model did not contemplate how, where, and what kind of data is being collected. Thus, the sub-dimension *Data Collection* was added.

Next, there were different opinions regarding the *Business Process* dimension. Expert 1 was more inclined to agree with the initial structuring and *Business Process* being a separate dimension, while Expert 2 explained that he sees it more as a sub-dimension of *Organisation*. While both views can exist, business process management is a discipline in operations management, so it is logical to include it under the Organisation dimension. Moreover, Expert 1 argued that decision making is a part of Business Processes, while Expert 2 suggested renaming it to decision-making process. Indeed, decision making is also a process in its nature, so it makes sense to discuss it in the business process sub-dimension. This remark also supports the previous modification of including business processes under organisation, because there is a strong link to other sub-dimensions in this dimension.

Moving on to the sub-dimension Culture. Expert 1 had a strongly opposing view to the inclusion of this sub-dimension in the model. He claimed that it brings unnecessary vagueness to it. However, Expert 2 approved this sub-dimension and discussed how in reality different cultures in the company call for different approaches and efforts in the IoT adoption, and that it does indeed impact this process. The literature analysis (see Section 4.2) also confirms that organisational culture is highly important and its transformation is an essential point of the adoption process. Therefore, sub-dimension Culture remains in the model. It is important to note, however, that it was renamed to culture of change to better reflect the content of this sub-dimension, based on the remark of Expert 2. Similarly, the sub-dimension IoT Team was renamed to IoT Implementation Support Team for the same reason.

Finally, the experts were asked about their opinion on the importance of reflecting business model transition in the model and how it should be carried out. Both experts agreed that it is a valid topic in the IoT adoption process. However, they explained that it is not limited to transition, but includes other possible business model modifications as well. Expert 1 stated that he would not include business model transition as a separate dimension. Similarly, Expert 2 did not mention its inclusion separately but instead proposed to explain it in the Strategy sub-dimension.

The final model consists of four dimensions and twelve sub-dimensions over five maturity levels. The final model is presented graphically in Figure 2. Novel dimensions, which are not found in any of the identified existing maturity models, are coloured in orange.

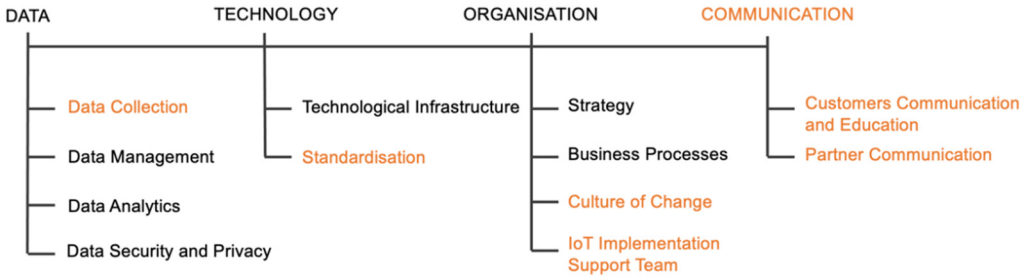

Figure 2. Final maturity model.

After the model refinement process was complete, the definition of dimensions, sub-dimensions, as well as the definitions of maturity across the levels were developed together with the experts. Model dimensions definitions are as follows:

Data: measures the organisation's capability in collecting, managing, analysing, obtaining insights, and extracting value from the IoT data.

Technology: measures the degree to which the organisation is equipped with the technological components and systems integration enabling the IoT implementation, and how IP standardised they are.

Organisation: measures the IoT adoption capacity from the business and managerial perspective within the organisation, in particular, its capability to address and exploit the generated value.

Communication: assesses the organisation's communication with its customers, business relations, and other external parties involved in the IoT adoption process.

The definitions of sub-dimension and maturity capabilities across the levels are presented in Table 2.

Table 2. Final maturity model.

Sub-Dimension	Sub-Dimension Definition	Level 0 Non-Existent	Level 1 Initial/Ad Hoc	Level 2 Repeatable but Intuitive	Level 3 Managed and Measurable	Level 4 Optimal and Robust
			Data Dimension			
Data Collection	Describes how well understood and defined are the sources, methods, the way of working, as well as the data quality and frequency of data collection.	Data collection is very limited and person dependent. It is performed in a random or reactive manner. The collected data is very lacking and incomplete.	An incomplete data collection process exists, but it is not documented, not standardised, and not planned in frequency terms. A lot of necessary data are not being collected.	The data collection process is well-defined, procedures are partially documented but still person-dependent, built from the bottom-up. Necessary data is occasionally not being collected.	Data collection is systemised, planned and organised. It is defined with goals in mind that are being measured and tracked. All necessary data is being collected. Algorithms to track the consistency of collected data are in place and can quickly detect if some data is not being collected.	Level 3 consistently in place for a longer period in time, hardened, and in continuous mode of improvement and external benchmarking.
Data Management	Describes how well understood and defined are the methods, the way of working in the regard of data storage, archiving, retention and integrity.	Data storage and management planning is non-existent and ad hoc. Very poor data quality.	Storage takes place in a coordinated way, but is lacking long-term process. Data quality needs considerable improvement.	Procedures have been defined to solve emerging storage problems without overall long-term system architecture. Average level of data quality is ensured.	Bottom-up data management procedures have been defined and optimised for short-term and longer-term system requirements. High data quality is ensured.	Level 3 is consistently in place for a longer period in time, hardened, and in continuous mode of improvement and external benchmarking.
Data Analytics	Measures the capabilities of the company and their systems in performing data processing and analysis, application of support programs and AI for value extraction and subsequent alert generation/signalling.	The company performs data processing and analysis in a rudimentary way.	Data processing and analysis is reactive and person-dependent. Support programs are not integrated. and alerts are not generated. No valuable insights are systematically extracted.	Data processing and analysis is consistent, but not performed in a standardised manner. Basic support programs are integrated. Although alerts are generated, they are not always correct and reliable. Valuable insights are extracted, but are occasional and are not systematically applied in decision making.	Data processing and analysis is systematic and standardised. Advanced support programs, including AI are integrated. Alerts are correctly generated and reliable. Signalling errors are rather an exception, and are quickly tracked and eliminated. Valuable insights are extracted, and are systematically applied in decision making.	Level 3 is consistently in place for a longer period in time, hardened, and in continuous mode of improvement and external benchmarking.
Data Security and Privacy	Describes the degree to which the company implements necessary data security measures and complies with the data privacy regulations.	No specific data security and privacy considerations in place.	Data security and privacy considerations are present, but are not consistent. Data access levels are not clearly defined and there is compliance with privacy regulations on some topics.	Data security measures within the company are defined and followed, but documentation is not complete. Data privacy regulations are followed in most cases.	Data security measures within the company are defined, documented, and followed. Data privacy regulations are consistently followed.	Level 3 is consistently in place for a longer period in time. Data security standards are continuously improved and compliance with data privacy regulations is monitored.
			Technology Dimension			
Technological Infrastructure	Describes the presence of necessary elements in the end-to-end chain such as components, IP networking, storage, computing and back-up power to support the IoT solution adoption.	No infrastructure to enable the IoT adoption.	The most elementary and basic technological infrastructure is put in place to cover some basic needs of IoT adoption. Some sensors are doing measuring for local situations and simple control loops. Storage and computing power are limited. Back-up solution is not very reliable. No E2E IP network in place.	Technological infrastructure covers multiple needs of IoT adoption, but does not realise its full potential. Some storage and computing power are available to perform basic tasks. Back-up solution mostly reliable, preserving the majority of data in case of a crash. E2E IP network in place.	Technological infrastructure realises the full potential of IoT adoption in the company. Systems are interconnected. Storage is able to accommodate constantly growing amounts of data. Computing power is sufficient to meet the needs. Back-up solutions are reliable, such that no data is lost in case of a crash. E2E IP network and platform in operation.	Level 3 is consistently in place for a longer period in time. Technological infrastructure is in continuous mode of improvement. Industry trends and best practices are constantly being monitored to expand the potential of the IoT adoption in the company.

Table 2. *Cont.*

Sub-Dimension	Sub-Dimension Definition	Level 0 Non-Existent	Level 1 Initial/Ad Hoc	Level 2 Repeatable but Intuitive	Level 3 Managed and Measurable	Level 4 Optimal and Robust
Standardisation	Describes the use of standardised hardware, software, interfacing, system development, data modelling, and representation.	No standardisation practices present.	Some practices in the use of hardware, software, interfacing are standardised, but not systematic. Data modelling and data representation are not consistent. The IP network is not integrated.	Hardware, software, interfacing is adhering to the standardised solution. Data modelling and representation are conducted in a consistent manner. Single integrated IP network is present.	Hardware, software, interfacing is adhering to the standardised solution. Data modelling and representation is conducted in a consistent manner. All necessary documentation is in place. Single integrated IP network is in place. Performance is measured and tracked.	Level 3 is consistently in place for a longer period in time, hardened, and in continuous mode of improvement and external benchmarking. The company is actively engaged in partner ecosystems.
			Organisation Dimension			
Strategy	Describes organisation's understanding of the purpose and possible gain of IoT, translated in short-term and long-term objectives and implementation steps, as well as the appropriate business model transformations.	The adoption of IoT does not have any strategic considerations.	A limited understanding of the purpose and possible gain of the IoT adoption exists. Related business opportunities and/or business needs are being considered. There are no clear business objectives.	The purpose of and gains from the IoT adoption are understood, and translated into business objectives. Implementation is not documented and highly relies on the knowledge of individuals.	IoT adoption has a solid strategic foundation. Long-term and short-term SMART objectives are set, and implementation plans developed and documented. Business model is transformed accordingly. The performance is measured.	Level 3 is consistently in place for a longer period in time. Industry trends are constantly being monitored. Sustainable business model is developed and implemented.
Business Processes	Describes the alignment of IoT with the business processes, as well as the degree to which phase-related decision making is driven by the IoT insights.	Business processes design and execution is performed with no consideration for IoT. Decision making is not driven by IoT insights.	Opportunities for business processes improvement with IoT in mind are identified and partially in place. Redesign of the business processes is taking place. Decisions are made on the basis of individual's knowledge.	Business processes are designed to be aligned with IoT implementation process. IoT insights are considered in decision making, but still impacted by the judgement of individuals.	Business processes are fully implemented leveraging full IoT capability. Decision making is consistently driven by the IoT insights, and fully documented.	Level 3 is consistently in place for a longer period in time. Business processes are in continuous mode of improvement. Decision making is completely independent.
Culture of Change	Describes employees' attitude towards IoT adoption, change management, goal alignment and communication.	There is no knowledge about IoT and no interest in applying it.	Information on IoT adoption is communicated poorly, with no clear connection to the goals of the organisation or the benefits it brings. Employees have limited knowledge on IoT, with only the minority being open to change.	Relevant knowledge about IoT and its adoption is openly shared within the organisation. Benefits and goals of the adoption initiative are clearly communicated. Employees have general knowledge about IoT and are mostly open to change.	Open knowledge culture is present. Customer centric approach is a driver of changes. Employees support the IoT adoption initiative. Training on IoT is provided to employees where relevant.	Level 3 is consistently in place for a longer period in time. Employees are knowledgeable about IoT and propose improvements. Organisation constantly reassesses its training to stay up to date with the IoT trends.
IoT Implementation Support Team	Describes the capabilities of the company's IoT implementation team, including its structure, team competencies, reporting, and accountability.	No separate team is formed to manage the IoT adoption.	Separate team is formed to manage the IoT adoption. Its structure is not balanced, and a lot of key competencies are lacking. Results are not consistent, and team accountability is poor.	There is some disbalance in the dedicated team structure, e.g., with people sometimes having to take on responsibilities beyond their usual expertise. Some key competencies are missing. Results are consistent, although team accountability is somewhat lacking.	Team structure is well balanced, with everyone focused on their area of work. All key competencies are present. Results are consistent, and team accountability is good. Working standards are documented and the performance is measured against them.	Level 3 consistently in place for a longer period in time. Team members are constantly looking to improve their competencies to be up to date with the industry best practices.

Table 2. *Cont.*

Sub-Dimension	Sub-Dimension Definition	Level 0 Non-Existent	Level 1 Initial/Ad Hoc	Level 2 Repeatable but Intuitive	Level 3 Managed and Measurable	Level 4 Optimal and Robust
			Communication dimension			
Customers Communication and Education	Describes how the company communicates with its customers about the IoT adoption as well as the customers' attitude towards IoT and trust in the company.	There is no understanding of change in customers' needs and wants under the rapid digitalisation and technological innovation process. No communication is established with customers about the IoT adoption within the company. Customers do not understand the IoT solution.	The company understands the change in customers' needs and wants, but is not able to establish a clear connection with how IoT adoption in the company can address them. Communication about IoT adoption is rather poor and unclear. Customers understand the basic idea of IoT but do not see how it benefits them, have high data security and privacy concerns and thus are reluctant to interact with the IoT solution.	The company has a clear understanding on how IoT can address the change in customers' needs and wants. A communication strategy is put in place to inform customers of the benefits of IoT. Information on the measures taken to ensure security and privacy of customers' data is transparent and easily accessible. Customers are well-educated about IoT and how it benefits them, and are open to interact with the IoT solution.	The company fully understands how IoT can address the change in customer's needs and wants and is constantly researching new ways to improve customer experience with the use of IoT. The company has set up a platform, where customers can learn about IoT in the company, including the benefits, opportunities, and security and privacy questions. The company actively communicates with customers and encourages them to share their experiences and concerns. Customers trust the company.	Level 3 consistently in place for a longer period in time. The company constantly monitors best in class case examples, industry trends and the overall innovation process to offer more secure and user-friendly experience.
Partner Communication	Describes how developed the company's communication with its partners, including the content, impact, and resulting agreements.	Communication is limited to what is operationally necessary to enable basic functioning of IoT within the company.	The company is actively communicating and collaborating with its direct and remote partners and looking to join a partner ecosystem.	The company is a member of the partner ecosystem, where an open exchange of knowledge and experience on IoT is present. The company and partners are working on becoming certified by recognised organisations in the areas of security and quality.	The company is a member of and contributing to the partner ecosystem, where an open exchange of knowledge and experience on IoT is present. The company has learned to utilise valuable information gained from this ecosystem to improve the IoT adoption in the company. Security and quality certification of recognised organisations are achieved.	Level 3 consistently in place for a longer period in time. The company has sufficient expertise and is respected and recognised within the ecosystem to participate in joint initiatives for the improvement of ways of working with IoT. The company is perceived as a reference company.

Note: This model is a general model, depending on the type of company and type of business, business-specific additions can be included.

8. Comparison with Other IoT Maturity Models

This section aims to provide a comparison of the developed model and the maturity models that have been built for IoT (Section 2). Table 3 shows an overview of this comparison highlighting in yellow the (sub-)dimensions that are not present in any of the compared models.

Table 3. Models Comparison.

Maturity Model for IoT Adoption by B2C Companies	Supply Chain Systems Maturing Towards the Internet of Things (IoT)—[8]	IoT Solutions Maturity Model—[13]	Integrated IoT Capability Maturity Model—[14]	Gartner's IoT Maturity Assessment—[16]	TDWI Readiness Model for IoT—[17]	Axeda's Connected Product Maturity Model—[18]	The IoT Technological Maturity Model—[7]	Maturity Model for IoT in Retail Industry—[19]
Data	x				x			x
Data Collection								
Data Management		x						x
Data Analytics		x	x		x			x
Data Security and Privacy								x
Technology		x	x	x			x	x
Technological Infrastructure	x				x			x
Standardisation								
Organisation					x			x
Strategy				x				x
Business Processes						x		x
Culture of Change								
IoT Implementation Support Team								
Communication								
Customers Communication and Education								
Partner Communication								

Notes: Model dimensions and sub-dimensions should be considered individually, i.e., X in the cell indicating a model dimension does not imply the inclusion of all respective sub-dimensions. In some cases, the names of (sub-)dimensions do not match exactly, but they are marked with an X nevertheless as the meaning of the (sub-)dimensions is the same.

Looking at the structure of the models, most importantly, dimensions and sub-dimensions, there are a couple of noticeable differences. Originally, it was found that technology, data management and analysis, and organisational culture are the most frequent dimensions present among the studied maturity models. As compared to the data management and analytics dimension, the final model refines the Data dimension with sub-dimensions Data Collection, Data Management, Data Analytics, and Data Security and Privacy. This more granular subdivision is due to the fact that in the context of IoT studies, the topic of data and its related terms should be handled very sensibly. Therefore, a clear distinction between the terms "collection", "management", "analytics" of data has been made. Because this clear distinction was missing in the other models, it might have been unclear exactly what kind of processes must be implemented in order to progress to the higher level of maturity of the Data dimension. Such change invites a more careful and serious towards data handling in the companies that wish to improve their maturity of IoT adoption.

Furthermore, there is a difference regarding the Organisational Culture dimension. What is meant by it, in the final model is represented by the sub-dimension Culture of Change. It allows for a more narrowed-down and concrete look at the question of cultural change in the organisation, and particularly its employees' attitude towards and knowledge about IoT, as well as how well they are managed. In such a manner, other irrelevant to IoT adoption process factors typically included in the discussion on organisational culture are filtered out.

Finally, another major change present in the final model as compared to the eight others is the addition of the Communication dimension. Communication with all stakeholders involved in and/or affected by the IoT adoption in the organisation was found to be a significant factor in the success of the adoption efforts. While the other eight models mainly included only internal processes in the maturity assessment, with the exception of the Customer feedback parameter in the IoT Solutions Maturity Model, the newly proposed model also accounts for external factors, such as an organisation's partners and clients. This addition allows for a more complete assessment of the IoT adoption maturity.

9. Conclusions and Further Work

The aim of this research was the development of the maturity model for IoT adoption in the companies operating in the B2C market. Two research questions guided the direction of this research:

R1: How can B2C organisations assess their current position in the IoT adoption process?

R2: How can B2C organisations achieve the next maturity level of the IoT adoption?

Considering the lack of IoT adoption maturity models specifically designed for B2C companies, this paper attempted to create one and fill this gap. In this regard, besides studying the IoT implementation in general, a considerable amount of time was also spent on studying the perspective of customers in this process and reflecting it in the major pillars of the model. As a result, the maturity model includes a separate sub-dimension describing the attitude and trust of customers towards the IoT adoption and the company, as well as the communication strategy the company employs to positively influence these two parameters. It can be seen that only after putting major effort in communicating with and educating customers about the IoT solution the company implements, it can achieve a high level of IoT adoption maturity. What is more, the B2C-specific characteristics are present in the sub-dimension Culture of Change. Here, high levels of IoT adoption maturity are only achievable after the customer-centric approach becomes the main driver of changes. Such transformations appear to be even more relevant in the present context because, ultimately, having high capabilities in the areas of data collection, management, and analytics allows a company to understand customer behaviour very well and build its business strategy around it. These two characteristics are what differentiates the IoT adoption maturity model developed in this research from the others. Accounting for the customer perspective on top of the essential IoT implementation factors usually present in existing maturity models will hopefully make the IoT adoption process for B2C companies more complete and effective.

Another distinctive factor of this model lies in its development methodology. Model dimensions and sub-dimensions identification relies not only on scientific sources but also on the opinions of industry experts and real successful implementation cases. The use in the model building of such a combination of practical experience and proven scientific theories makes it valuable for the actual companies because they can be sure that the content of this model lies not far from what they usually deal with in their business operations. Moreover, the validation of the model and development of maturity definitions across the levels was performed in close collaboration with the experts. This approach also contributed to the applicability of the developed model in the business world.

The answer to the research questions is, ultimately, the maturity model itself. Companies can use it as a tool to both assist them in the assessment of their current IoT adoption maturity level, and as a guide for the improvement in their position across the key areas. Achieving the characteristics of the succeeding maturity level is what the companies that wish to improve their maturity should work towards. At the same time, it is important to keep in mind that while this model attempts to provide a complete view on all areas involved in and important for IoT adoption, the actual complexity of this process might stretch beyond it, involving other uncovered factors and relationships. Therefore, it ought to be used as a guide for IoT adoption and not as an easy step-by-step action plan, which guarantees a successful end result.

This research is subject to a couple of limitations. The most major one—that in the end might have limited the validity threads of the paper—is communication and collaboration with the industry. Finding experts to participate in the research turned out to be difficult, even though the proper planning was present. With the global COVID-19 pandemic happening during the time of executing this research and companies facing related difficulties, it is possible that the low response rate and delays in communication with the experts are attributed to this. Having said that, a total of two experts participating in the research might be too low considering the importance of the practically oriented model development and how much the experts are involved in this process. Another limitation

also related to pandemic-induced communication impediments is that the interviews were not conducted with the consumers of IoT solutions. If conducted, they might have revealed valuable insights for the model development, especially considering the B2C focus of this maturity model.

Future research can definitely expand the expert panel to increase the accuracy and validity of the results. Moreover, professionals from B2C companies, who do not specialise in IoT, for example, HR managers or marketers, can also be invited to participate in the research to provide their view on the adoption process in the specific departments. Another possibility for future research is to study whether the different B2C market segments lead to significant differences in the IoT adoption maturity model. Finally, statistical research based on the development of hypotheses may be conducted in order to validate the model dimensions.

Supplementary Materials: The following supporting information can be downloaded at: https://www.mdpi.com/article/10.3390/app12030982/s1, Supplementary Materials S1: Interview protocol and interview questions; Supplementary Materials S2: Notes from the first series of interviews; Supplementary Materials S3: Notes from the second series of interviews; Supplementary Materials S4: Initial model.

Author Contributions: Funding acquisition, E.S.A.; methodology, O.K. and E.S.A.; supervision, E.S.A.; visualization, O.K.; writing—original draft, O.K.; writing—review and editing, O.K. and E.S.A. All authors have read and agreed to the published version of the manuscript.

Funding: Funded by the FWO (Fonds Wetenschappelijk Onderzoek) research project fundamental research G0C6721N.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: The data presented in this study are available in the attachments.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Lueth, K. State of the IoT 2018: Number of IoT Devices Now at 7B—Market Accelerating. 2018. Available online: https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/ (accessed on 6 October 2019).
2. Leonard, P.G. Business-to-Consumer IoT Services, Consumer Protection and Regulation. *SSRN Electron. J.* **2017**. [CrossRef]
3. Klötzer, C.; Pflaum, A. Toward the development of a maturity model for digitalization within the manufacturing industry's supply chain. In Proceedings of the Hawaii International Conference on System Sciences (HICSS) 2017, Hawaii County, HI, USA, 4–7 June 2017.
4. Paulk, M.C.; Curtis, B.; Chrissis, M.B.; Weber, C.V. Capability maturity model, version 1.1. *IEEE Softw.* **1993**, *10*, 18–27. [CrossRef]
5. Ganzarain, J.; Errasti, N. Three stage maturity model in SME's toward industry 4.0. *J. Ind. Eng. Manag. (JIEM)* **2016**, *9*, 1119–1128.
6. Gökalp, E.; Şener, U.; Eren, P.E. Development of an Assessment Model for Industry 4.0: Industry 4.0-MM. In Proceedings of the International Conference on Software Process Improvement and Capability Determination, Tessaloniki, Greece, 9–10 October 2017; Springer: Cham, Germany, 2017; pp. 128–142.
7. Jæger, B.; Halse, L.L. The IoT technological maturity assessment scorecard: A case study of norwegian manufacturing companies. In Proceedings of the IFIP International Conference on Advances in Production Management Systems, Hamburg, Germany, 3–7 September 2017; Springer: Cham, Germany, 2017; pp. 143–150.
8. Katsma, C.P.; Moonen, H.M.; van Hillegersberg, J. Supply Chain Systems Maturing Towards the Internet-of-Things: A Framework. In Proceedings of the Bled eConference, Bled, Slovenia, 12–15 June 2011; p. 34.
9. Leyh, C.; Bley, K.; Schäffer, T.; Forstenhäusler, S. SIMMI 4.0-a maturity model for classifying the enterprise-wide it and software landscape focusing on Industry 4.0. In Proceedings of the 2016 Federated Conference on Computer Science and Information Systems (Fedcsis), Gdansk, Poland, 11–14 September 2016; pp. 1297–1302.
10. Schumacher, A.; Erol, S.; Sihn, W. A maturity model for assessing Industry 4.0 readiness and maturity of manufacturing enterprises. *Procedia CIRP* **2016**, *52*, 161–166. [CrossRef]
11. Weber, C.; Königsberger, J.; Kassner, L.; Mitschang, B. M2DDM—A maturity model for data-driven manufacturing. *Procedia CIRP* **2017**, *63*, 173–178. [CrossRef]
12. Westermann, T.; Anacker, H.; Dumitrescu, R.; Czaja, A. Reference architecture and maturity levels for cyber-physical systems in the mechanical engineering industry. In Proceedings of the 2016 IEEE International Symposium on Systems Engineering (ISSE), Edinburgh, UK, 3–5 October 2016; pp. 1–6.

13. Rawal, D. *IoT Solutions Maturity Model. IoT Solutions Maturity Model*; Tech Mahindra: Pune, India, 2018. Available online: https://vdocuments.net/iot-solutions-maturity-model-tech-mahindra-papersneiot-solutions-maturity.html (accessed on 19 October 2019).
14. Vachterytė, V. Towards an Integrated IoT Capability Maturity Model. Bachelor's Thesis, University of Twente, Twente, The Netherlands, 2016.
15. Bugeja, J.; Vogel, B.; Jacobsson, A.; Varshney, R. IoTSM: An end-to-end security model for IoT ecosystems. In Proceedings of the 2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kyoto, Japan, 11–15 March 2019; pp. 267–272.
16. Wallin, L.; Jones, N.; Kleynhans, S. *How to Put an Implementable IoT Strategy in Place (Report No. G00275309)*; Gartner Inc.: Stamford, CT, USA, 2017. Available online: https://www.gartner.com/imagesrv/research/iot/pdf/iot-275309.pdf (accessed on 8 November 2019).
17. Halper, F. *TDWI IoT Readiness Guide: Interpreting Your Assessment Score*; TDWI: Renton, WA, USA, 2016. Available online: https://tdwi.org/whitepapers/2016/08/tdwi-iot-readiness-guide.aspx (accessed on 28 September 2019).
18. Axeda Corporation. *Achieve Innovation with Connected Capabilities: Connected Product Maturity Model [White Paper]*; Axeda Corporation: Needham Heights, MA, USA, 2014. Available online: https://www.yumpu.com/en/document/read/51211187/connected-product-maturity-model-axeda-blog (accessed on 11 November 2019).
19. Serral, E.; Vander Stede, C.; Hasić, F. Leveraging IoT in Retail Industry: A Maturity Model. In Proceedings of the 2020 IEEE 22nd Conference on Business Informatics (CBI), Antwerp, Belgium, 22–24 June 2020; Volume 1, pp. 114–123.
20. Felch, V.; Asdecker, B.; Sucky, E. Maturity models in the age of Industry 4.0–Do the available models correspond to the needs of business practice? In Proceedings of the 52nd Hawaii International Conference on System Sciences, Grand Wailea, Maui, 8–11 January 2019.
21. Becker, J.; Knackstedt, R.; Pöppelbuß, J. Developing maturity models for IT management. *Bus. Inf. Syst. Eng.* **2009**, *1*, 213–222. [CrossRef]
22. Microsoft. *IoT Signals. Summary of Research Learnings 2019*; Microsoft: Redmond, WA, USA, 2019. Available online: https://azure.microsoft.com/en-us/iot/signals/. (accessed on 28 December 2019).
23. Jalali, M.S.; Kaiser, J.P.; Siegel, M.; Madnick, S. The Internet of Things Promises New Benefits and Risks: A Systematic Analysis of Adoption Dynamics of IoT Products. *IEEE Secur. Priv.* **2019**, *17*, 39–48. [CrossRef]
24. Hsu, C.L.; Lin, J.C.C. An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives. *Comput. Hum. Behav.* **2016**, *62*, 516–527. [CrossRef]
25. Lee, I.; Lee, K. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons* **2015**, *58*, 431–440. [CrossRef]
26. Friedman, T. *Gartner Data & Analytics Summit. Gartner Data & Analytics Summit*; Gartner: Grapevine, TX, USA, 2018. Available online: https://www.gartner.com/en/webinars/3890780/what-the-internet-of-things-means-for-your-data-and-analytics-ca (accessed on 8 January 2020).
27. Bandyopadhyay, D.; Sen, J. Internet of things: Applications and challenges in technology and standardization. *Wirel. Pers. Commun.* **2011**, *58*, 49–69. [CrossRef]
28. Singh, S.; Singh, N. Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce. In Proceedings of the 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), Delhi, India, 8–10 October 2015; pp. 1577–1581.
29. Evans, H.I. Barriers to Successful Implementation of the Internet of Things in Marketing Strategy. *Int. J. Inf. Commun. Technol. Res.* **2015**, *5*. Available online: https://www.semanticscholar.org/paper/Barriers-to-Successful-Implementation-of-the-of-in-Evans/db74a33b899b83af437f80d46f7c68cdb209fbf7 (accessed on 20 December 2021).
30. Kamble, S.S.; Gunasekaran, A.; Parekh, H.; Joshi, S. Modeling the internet of things adoption barriers in food retail supply chains. *J. Retail. Consum. Serv.* **2019**, *48*, 154–168. [CrossRef]
31. Al-Momani, A.M.; Mahmoud, M.A.; Sharifuddin, M. Modelling the adoption of internet of things services: A conceptual framework. *Int. J. Appl. Res.* **2016**, *2*, 361–367.
32. Gao, L.; Bai, X. A unified perspective on the factors influencing consumer acceptance of internet of things technology. *Asia Pac. J. Mark. Logist.* **2014**, *26*, 211–231. [CrossRef]
33. AlHogail, A. Improving IoT technology adoption through improving consumer trust. *Technologies* **2018**, *6*, 64. [CrossRef]
34. Kranz, M. *Building the Internet of Things: A Project Workbook*; ICGtesting: Hoboken, NJ, USA, 2018.
35. Caro, F.; Sadr, R. The Internet of Things (IoT) in retail: Bridging supply and demand. *Bus. Horiz.* **2019**, *62*, 47–54. [CrossRef]
36. Slama, D.; Puhlmann, F.; Morrish, J.; Bhatnagar, R.M. *Enterprise IoT: Strategies & Best Practices for Connected Products & Services*; O'Reilly: Beijing, China, 2016; pp. 20–22.
37. Maliping. 2019 2nd International Conference on Computer Information Science and Artificial Intelligence. *J. Phys. Conf. Ser.* **2019**, *1453*, 25–27. Available online: https://iopscience.iop.org/article/10.1088/1742-6596/1453/1/012098 (accessed on 18 January 2020).
38. Anciaux, L. Iot Project Management. IoT Factory. Available online: https://iotfactory.eu/iot-knowledge-center/free-report-iot-project-management/ (accessed on 28 January 2020).

39. Schuh, G.; Anderl, R.; Gausemeier, J.; Ten Hompel, M.; Wahlster, W. (Eds.) *Industrie 4.0 Maturity Index: Managing the Digital Transformation of Companies*; acatech: Munich, Germany, 2017.
40. Büyüközkan, G.; Göçer, F. Digital Supply Chain: Literature review and a proposed framework for future research. *Comput. Ind.* **2018**, *97*, 157–177. [CrossRef]
41. Yong Wee, S.; Siong Hoe, L.; Kung Keat, T.; Check Yee, L.; Parumo, S. Prediction of user acceptance and adoption of smart phone for learning with technology acceptance model. *J. Appl. Sci.* **2011**, *10*, 2395–2402.
42. Abu, F.; Jabar, J.; Yunus, A.R. Modified of UTAUT theory in adoption of technology for Malaysia small medium enterprises (SMEs) in food industry. *Aust. J. Basic Appl. Sci.* **2015**, *9*, 104–109.
43. Davis, F.D. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Q.* **1989**, *13*, 319–340. [CrossRef]
44. Shackelford, S.J.; Proia, A.A.; Martell, B.; Craig, A.N. Toward a global cybersecurity standard of care: Exploring the implications of the 2014 NIST cybersecurity framework on shaping reasonable national and international cybersecurity practices. *Tex. Int'l LJ* **2015**, *50*, 305.
45. Shen, L. The NIST cybersecurity framework: Overview and potential impacts. *Scitech Lawyer* **2014**, *10*, 16.
46. SIA Partners. *The Internet of Things in Transportation—Port of Hamburg Case Study*; Sia Partners: Paris, France, 2016. Available online: https://transport.sia-partners.com/20160930/internet-things-transportation-port-hamburg-case-study (accessed on 20 March 2020).
47. Cognizant. *IoT Enables Data Insights and Innovation at Heavy Equipment Company*; Cognizant: Teaneck, NJ, USA, 2020. Available online: https://www.cognizant.com/case-studies/pdfs/telemetry-solution-for-heavy-equipment-manufacturer-codex2996.pdf (accessed on 18 March 2020).
48. Cognizant. *Retail IoT Solution Connects Analytics and Building Assets to Boost Efficiency and Reduce Waste*; Cognizant: Teaneck, NJ, USA, 2019. Available online: https://www.cognizant.com/case-studies/iot-solution-retail-refrigeration (accessed on 18 March 2020).
49. ISACA. *Cobit 2019 Framework: Introduction and Methodology*; ISACA: Schaumburg, IL, USA, 2018. Available online: https://www.isaca.org/resources/cobit (accessed on 22 January 2020).