information

Article

Openness and Security Thinking Characteristics for IoT Ecosystems

Bahtijar Vogel [1,*], Miranda Kajtazi [2], Joseph Bugeja [1] and Rimpu Varshney [3]

[1] Internet of Things and People Research Center, Department of Computer Science and Media Technology, Malmö University, 20506 Malmö, Sweden; joseph.bugeja@mau.se

[2] Department of Informatics, Lund University, 22363 Lund, Sweden; miranda.kajtazi@ics.lu.se

[3] Department of Security, Booking.com, 1000 BP Amsterdam, The Netherlands; rimpu.varshney@gmail.com

* Correspondence: bahtijar.vogel@mau.se

Received: 31 October 2020; Accepted: 25 November 2020; Published: 2 December 2020

Abstract: While security is often recognized as a top priority for organizations and a push for competitive advantage, repeatedly, Internet of Things (IoT) products have become a target of diverse security attacks. Thus, orchestrating smart services and devices in a more open, standardized and secure way in IoT environments is yet a desire as much as it is a challenge. In this paper, we propose a model for IoT practitioners and researchers, who can adopt a sound security thinking in parallel with open IoT technological developments. We present the state-of-the-art and an empirical study with IoT practitioners. These efforts have resulted in identifying a set of openness and security thinking criteria that are important to consider from an IoT ecosystem point of view. Openness in terms of open standards, data, APIs, processes, open source and open architectures (flexibility, customizability and extensibility aspects), by presenting security thinking tackled from a three-dimensional point of view (awareness, assessment and challenges) that highlight the need to develop an IoT security mindset. A novel model is conceptualized with those characteristics followed by several key aspects important to design and secure future IoT systems.

Keywords: IoT; ecosystem; openness; security; privacy; awareness; assessment; challenges; security thinking; model; design

1. Introduction and Background

The Internet of Things (IoT) market is predicted to grow from an installed base of 20 billion devices in 2017, to 30.7 billion devices in 2020 and 75.4 billion in 2025 [1–3]. Within less than a decade, a new infrastructure for online sociality and creativity has emerged, which forms a new layer of the digital infrastructure, through which people have started to organize their lives. Such infrastructures are becoming new digital ecosystems where different platforms and devices influence human action and interaction not always with the best output [4]. However, as our dependency on digital ecosystems increases that include Artificial Intelligence (AI) and Machine Learning (ML) techniques, together with the number of devices and people getting connected to these ecosystems, the responsibility to provide the right security and privacy measures becomes a serious concern, which we must not take lightly.

Currently, proprietary technologies, e.g., industry standards for communication, have been extensively deployed throughout multiple IoT systems and devices, and often they are closed and fragmented [5,6]. In the smart living domain, this was for instance demonstrated by Nikayin et al. [7] who, in their review of service platforms—these can be seen as hardware, software, network infrastructure or a combination of these [7]—indicated that the majority of service platforms intended for the smart home are closed allowing access to information only by platform providers. Furthermore, fragmentation exists, as it is challenging to maintain platform compatibility, when adaptation, evolution and security are the main characteristics that should portray the IoT systems.

For IoT practitioners to build systems in a more standardized way, there is a need for an open approach [6]. Big industry actors (such as Samsung) have already announced the need "for greater openness and collaboration across industries to unlock the infinite possibilities of the Internet of Things" [8]. Openness is usually characterized by transparent access to information, other resources, collaborative participation, and after all is about opening up [9]. Openness is a de-facto trend in the IoT domain, whereas its interpretation relies on different stakeholders view and their domains [10]. Moreover, values of openness via Blockchain smart contracts are particularly encouraged as it can help reducing the surveillance threats while improving the trust to IoT ecosystems [11].

Openness in IoT systems offer multitude of benefits [10], but security is never assured [12,13]. Security and privacy goals are at the top of the agenda for the industry, yet a growing number of smaller IoT vendors, typically startups, whose core competence does not focus on security, brings a bigger challenge to set-up a secure IoT infrastructure [14–16]. As an example, if a traditional hardware manufacturing company enables internet connectivity on their product, they can accomplish this with a small group of software developers. However, they might not necessarily have the security expertise and budget allocated to conduct security processes such as threat modelling, risk assessment and security audits. This can result in poor quality and insecure systems that could be relatively easily exploited by hackers due to several security vulnerabilities they may contain [17,18].

Today, we should strive to develop IoT technologies with the right mindset where security and privacy should be key. Highlighting the inevitable presence of IoT, in this study, the goal is to prioritize openness and security as mandatory characteristics for the IoT ecosystems. In this paper, we propose a model for IoT practitioners and researchers on how to use security thinking in parallel with open IoT technological developments. This paper is an extension of the work related to openness and security aspects based on our previous research efforts [6,19,20].

Some of the main contributions can be summarized as:

- First, we identify a set of *openness* and *security thinking* characteristics important for IoT ecosystems, (a) *openness* encompasses open architectures followed by a number of important aspects such as open standards, open data, open Application Programming Interfaces (APIs), open processes, and open source; (b) *security thinking* encompasses awareness, assessment and challenges that are needed to develop an IoT security mindset.
- Second, we propose a novel model which is conceptualized with the identified characteristics followed with several key aspects important to design and secure future IoT systems. Our conceptualized model emphasizes the human in the loop concept that would help to easily understand the emerging needs as design principles for IoT ecosystems in a more open and secure way.
- Finally, we show that novelty and risks concurrently target security in the IoT, and thus the importance of the three identified dimensions: *awareness*, *assessment* and *challenges*, together with a number of identified aspects uplifting continuous security thinking.

In the next section, we motivate both *openness* and *security thinking* as key concepts and models that were developed to target the IoT ecosystems. We discuss our approach and settings of the study. We then focus on the state-of-the-art, particularly in relation to security in IoT. In addition, we provide empirical input by understanding how practitioners view IoT openness and security. We identify three key security dimensions and related aspects. Followed by the research approach and results from the state-of-the-art in IoT security, we then bring the empirical study data. We finally conclude the paper.

2. Motivation and Related Work

Mark Wieser's seminal work on ubiquitous computing, considered the precedent of what we frame today as the IoT, proposed the idea of technology working in the background while its actions come in the forefront [21]. Today, we strive to develop such technology through IoT, where security and privacy are prioritized. According to Agarwal and Dey [22], these aspects must be tackled from the ground-up. However, aspects like extreme heterogeneity lack standardization for the openness [6] and ineffectiveness of traditional methods of security [22] are a constant target for finding the right security solutions. Challenging IoT security from a security thinking perspective puts security in the spotlight for continuous efforts among practitioners and researchers to improve it [20]. In the subsections below, we motivate the openness aspects based on our previous research efforts [6,19], while extending it with security thinking [20], and we believe that both are important characteristics for IoT ecosystems.

2.1. The Need for Openness of IoT as Design Principles

Architectural aspects are elementary and play a pivotal role for IoT ecosystems. Particularly, design-time and run-time undergo a constant change in IoT Architecture because these two elements are characterized by a dynamic mechanism [23]. In this dynamism, openness is problematic because it requires a better exploration to determine the development aspects tackled with transparency [6,24]. In this way, IoT ecosystems can rely on open architecture, for example when dealing with heterogeneous devices, and constantly new emerging requirements [6,24]. The open architecture can help to establish the very initial design and system settings that can express the architectural design characteristics as attributes or constraints for a system [6].

For IoT ecosystems to provide a platform that accommodate the open architecture approach, any developed e.g., application should proactively consider the open architecture approach to make sure that there is support for the continuous changes without affecting the behavior of an overall system. Figure 1 shows that the open architecture approach is characterized by flexibility, customizability, and extensibility. The figure also makes a set of design activities noticeable for which each property can facilitate the design of the architecture itself. In addition, the properties of ease and cost-effectiveness are connected to each of these characteristics. Then, the open architecture design principles can support the evolution of the IoT ecosystems by addressing the emerging requirements and the very changing needs of the stakeholders [6,24,25].

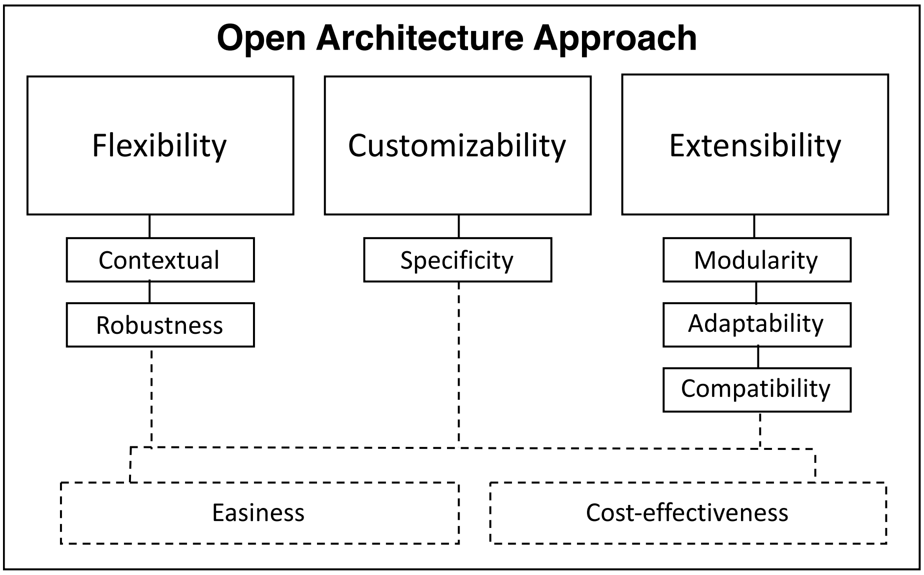

Figure 1. Open Architecture design principles conceptualized, adapted from [6].

Some of the main aspects of the open architecture design principles are its inherent characteristics, such as modularity, compatibility, easiness, cost-effectiveness, quality aspects related to performance, correctness of processes, and so on, together with the set of design time properties, namely [6,24,25]:

Flexibility characteristic, can enable solutions to be used by the users in a wide variety of settings and situations by easily addressing different user's requirements with minimum delays. The main properties of flexibility are: context, robustness, easiness and cost-effectiveness [6].

Customizability characteristic, can enable the users to easily customize features in the system and address their specific individual needs, usually without having access to the source code, thus reducing the deployment time. The main properties of customizability are: specificity, easiness and cost-effectiveness [6].

Extensibility characteristic, can offer easy integration possibilities with other systems and/or tools that takes into consideration future growth by expanding/enhancing the architecture with less costly upgrades. The main properties of extensibility are: adaptability, modularity, compatibility, easiness and cost-effectiveness [6].

Future steps should address questions regarding accommodating security as an additional characteristic within an open architecture approach for IoT ecosystems by further enhancing the reliability of IoT systems for the society.

2.2. The Need for Security Thinking

Challenging IoT security from a security thinking approach puts security in the spotlight for continuous efforts among practitioners and researchers to improve it. Security thinking is expressed in two forms. First, it refers to the technical measures the IoT practitioners take when developing an IoT system. IoT systems often expand with security and privacy considered as an afterthought [26] at the expense of lack of security expertise, cost-savings and time trade-off [15]. This should be carefully planned with an ethical use and development of IoT by investing significant resources also on the sociotechnical IoT aspects [27]. Second, it refers to progress towards a secured organizational culture often by ensuring employee training and education to influence and activate their thinking about information security [28]. Recent studies like Kajtazi et al. (2018) [29] and Moody et al. (2018) [28] show that security thinking is not developed enough in organizations from an employee point of view, a trend that has likely influenced the immature thinking of security development across IoT systems from the back-end perspective. Instead, organizations prioritize releasing their products to the market at the stake of security. Likewise, we argue that we should be striving for an IoT security thinking mechanism expressed in the two forms above, but following a consecutive order, first a proactive security mechanism during requirements, development and implementation, and then security awareness tactics. Echoing Lowry et al. [17], who stated that IoT is rewriting all the rules on how we once considered security, the IoT infrastructure will fail if we don't act proactively.

3. Research Approach

This study begins by formulating state-of-the-art concepts and models for openness and security in IoT. While some studies were not directly focusing on IoT per se, we included them by realizing that their input was key in strengthening security thinking for IoT developers, implementers and users. Scrutinizing the security literature from the IoT perspective to form the state-of-the-art, we observe that there are very few security insights from practitioners. In dealing with this challenge, we conducted a study driven by the semi-structured interview approach with six experts within the IoT field and from different IoT domains. This study uses the first-hand experience of six security and IoT practitioners from different organizations. Respondents' identifiers (R1–R6) alongside their corresponding details are presented in Table 1.

Table 1. Interviews with experts: their role and domains.

Respondent	Role	IoT Domains
R1	Security Architect	Mobile Communications
R2	Senior Architect	IoT Solutions
R3	Technology Leader	Industry Automation
R4	Technology Expert	Home Security
R5	Security Coach	Home Surveillance
R6	Security Expert	Data Security

Table 2 shows the interview questions that were used to interview the experts and practitioners in the domain of IoT. Details on how the interview guide was developed and the presentation of raw data from the interviewees can be found in [19,30].

Table 2. Interview questions.

IoT
Q1. What is your job role in your organization? Q2. What does Internet of Things mean to you? Q3. What are the properties associated with smart things? Q4. Are you aware of any general constraints in Internet of Things?
Security Awareness
Q5. What are your views on security of Internet of Things? Q6. What are your views on privacy of Internet of Things? Q7. What are the challenges or constraints in using existing security measures on Internet of Things?
Designing Open and Secure IoT Systems
Q8. How openness affects IoT (Flexibility, Customizability, and Extensibility)? Q9. What do you think considering security and privacy while designing IoT solutions is critical? Q10. Are you aware of any existing security mechanisms within your organization that can address challenges in Internet of Things? What measures can you suggest? Q11. Do you want to make any last statement for IoT community and developers?

4. Results and Discussion

In this section, a discussion of results from theoretical and empirical findings are highlighted. These results are mapped and discussed in the sections below in a summarized way. We discuss the results from designing open and considering security perspectives for IoT ecosystems, followed with a proposal for general security thinking in IoT.

4.1. Openness vs. Security

The results emphasize the *openness* aspects as an emerging trend [6,10,31,32]. However, we also need to point out that openness trends are adapted towards some of the openness aspects and IoT applications, for e.g., when it comes to the smart home, there are still a number of devices, such as: gateway/hub that feature a closed ecosystem or with some proprietary standards and APIs [33], whereas most of them are closed when considered from an industrial-based IoT systems [34].

IoT stakeholders are encouraged to make use of openness to benefit from its aspects of easiness, convenience and fast development that are often attributed to produce positive results with cost related savings [35]. Openness in general is about using open standards, open source, open APIs, open data, open layer [10], open processes and open architectures [6,24]. The heterogeneity aspects enabled by IoT devices and their emerging requirements demand the need for an open IoT architecture. Such an open architecture has the potential to ease the use of these devices by developers and end-users (e.g., in smart home context). Open architecture design principles, particularly flexibility, customizability, and extensibility, as well as ease and cost-effectiveness properties [6], can support the evolution of IoT ecosystems towards satisfying constantly evolving requirements.

In general, and despite the confidence that openness of IoT architectures brings with its characteristics of flexibility, customizability and extensibility, incorporating into those characteristics the importance of security and privacy as key design principles is central (R1, R4, and R6 and according to Table 1). If security and privacy continues to be neglected, the improper choices of openness aspects can lead to opening up for larger attacks into the IoT ecosystems (R6, R3, and R5). This is important to be considered, since openness allows for sharing and interoperability, as well as addressing the growth and maintainability of the system, increases the speed of development, and reduces developmental costs (R1, R3).

Our results show that it is crucial to have openness in IoT domain since it allows for better interoperability and transparency, often sharing of source code, data, interfaces and other technical and nontechnical artefacts. In addition, openness can support the IoT industry in terms of the growth, easier maintenance and speed of development (R1, R3). However, it is imperative to consider that security of IoT ecosystems should be an integral part of openness. In addition, security in this area is not just a need, but it becomes mandatory for a successful deployment and execution of an open IoT system (all respondents). This is mainly because often the open systems are by default seen as insecure. IoT ecosystems should prioritize considering security by design aspects (all respondents). To follow up on that, security aspects need to be addressed right from the start of the IoT design because they are rather harder to be implemented retroactively. Moreover, our results highlight that security should not be neglected during any design phase of the development lifecycle. In addition, since privacy is an integral part of security (R1, R5), IoT systems should also consider privacy by design aspects. The IoT industry needs to start thinking about open and secure IoT ecosystems as design principles from the very initial development phase.

The IoT ecosystems characterized by openness and diversity of technologies require serious reflections particularly related to security issues [36] (all respondents). Our results show that security begins with awareness and built-in security mindset [37] (R1, R4, R6). While we often find that security is an after thought, today's security approach should not be introduced after the product is deployed, but it rather needs to be integrated across all design and development stages (R4, R5). Therefore, security problems are no longer attributed to a 'tool or an implementation', but it is rather a 'people and process' issue (Respondent: R5). Thus, it is not solely technology that makes IoT ecosystems secure, but it is the development community, open processes and open approaches that are followed which make an IoT ecosystem secure [19].

These insights point towards IoT practitioners that need to consider deeper aspects by following more proactive security thinking approach when designing open and secure IoT systems [19].

4.2. Continuous Security Thinking

In the traditional view, a good security practice was likely achieved through effective technologies, policies, standards and procedures that intended to ensure the CIA-triad: confidentiality, integrity and availability. Confidentiality is seen as the prevention of unauthorized disclosure, integrity as the prevention of the unauthorized modification, and availability as the prevention of unauthorized withholding of data [38]. The CIA-triad has been extended over the years—e.g., the CIA+ to deal with network security attacks [39]. Nonetheless, the IoT domain poses additional aspects that are not covered by the mentioned models. Additionally, in IoT systems, new security requirements have arisen due to specific features, e.g., use of cloud technology and properties e.g., constrained resources, of IoT systems. Even if security and privacy must go hand-in-hand, there are often situations when the prior becomes a cause for concern for the former. For example, strengthening surveillance systems for a better security comes at the expense of privacy. In light of the aspects mentioned above, below we provide an overview of related studies by mapping with interview data while identifying and highlighting different security aspects (see details in Table 3).

IoT Awareness: Raising awareness for *data management* in terms of sensitive information in the IoT domain current practices is an important feature [40–42]. However, *training and education* require broader spectrum of stakeholders to be included, such as policy makers, regulators and the general public in order to raise such awareness regarding IoT challenges, risks and opportunities [37,43] (all respondents). More specifically, there is a need for *user awareness and security education* for both developers and users of smart products and services [44] (R5). The best way to keep security on users' attention is to offer continuous security awareness and education programs [45]. Because these smart products and services should be *designed-in security* concepts in mind [43,46] and at the same time dealing with *ethical concerns* in terms of bringing awareness to owners of IoT smart products related to the degree of privacy [47], *continuous education* for engineers and other stakeholders in IoT field is important for enabling life-long learning regarding security and privacy aspects likewise [27,37,45,48]. Additional features for organizing learning mechanisms, team building and knowledge management systems need to be provided in connection to *people and team management* aspects [49]. For raising awareness among IoT industry management and practitioners, there is a need for an adequate *legal framework* that would take the underlying technology into account [14]. This legal framework could be established by the legislator which can also be supplemented by the IoT industry according to their specific needs [14]. Furthermore, a legal framework could ensure stakeholders awareness and protection of subjects, e.g., when it comes to privacy breaches [50]. In order to place this framework into practice, *policy enforcement* as another feature of IoT security awareness aspect is important to be considered [51,52]. Security should be introduced in a form of *security as a process* aspect that would help with thinking about security from the initial design phase and throughout the development lifecycle (R5). Developers should understand the *context* of operation and then apply security patterns, mechanisms and tools that work for their team (all respondents). This is especially important in IoT as often it is not possible to state general practices or guidelines for designing secure IoT system (R1, R5). *Learn by observing* instead of reinventing the wheel is another aspect, as there is a need to look at the success models because often the problems IoT practitioners face are already encountered and solved in other mature industries (R5). *Addressing the digital divide* aspect deals with IoT practitioners that need to have larger responsibility for securing IoT users, mainly because of their various levels of understanding the security and privacy risks (R1, R6). Security is a continuous process, thus the *keep secure always* aspect could enable timely upgrades and updates of the system by issuing necessary and critical fixes (all respondents). Security fixes must be enforced on the IoT users to keep their system always secure (R6). *Plan for end-to-end security* should be designed and implemented addressing all the components of an IoT ecosystem, from the end-user to devices to network, and so on (R6).

IoT Assessment: Building trust in humans is an essential assessment item of security and privacy within the IoT field [51,53]. IoT devices need to be designed with *identity management* appropriate for the IoT environment [51,54,55] for e.g., in terms of maximizing data integrity and ensuring trust mechanisms [27]. Security risks can arise due to multiple reasons, e.g., unawareness of maliciously manipulated products or the lack of information on potential countermeasures [44]. In order to avoid certain vulnerabilities and risks, *risk management* is an important aspect of assessment in security in terms of threat modeling, code reviews, and various testing aspects such as white/black-box testing [37,43,46,56] (R5, R6). In this case, mitigation measures should also be considered by utilizing *security and privacy by design principles* [43,48,50,57] (all respondents). Having *trust management* usually helps to overcome the uncertainties and risks within the IoT environment [19,52,55] (R1, R2). *Auditing* is another important IoT feature [27]) (R5, R6). This feature is important as it leans more towards transparency when implementing the security of IoT devices [27]. In particular, auditing when done repeatedly against security standards, helps in building user trust [58]. In the end, *compliance* sets the frontal image of how assessment should be developed within the IoT infrastructure [20,27,43]. Having an IoT provider compliant to security standards may also contribute in attracting more users to use the provider services [58]. Assessment for IoT developers should let them think about necessary *tools and software assessment*. A security toolbox helps practitioners conduct e.g., threat modeling, architectural review, code review, and running automated security tests (R5). IoT stakeholders should think about *data assessment* aspects as well, in order to assess data for its correctness, trustworthiness, and reliability (R1, R6) [19,43,57].

IoT Challenges: Many IoT devices used today were originally designed in *closed* way for non-internet use and with *proprietary* code, and often using weak protocols and practices [6,41–43]. Even though many *standardization* bodies together with industry tried to provide solutions for security and privacy aspects [42,43], standardization in IoT still remains as a continuous challenge [44] (R2, R6). *IoT complexity* makes it almost impossible to realize secure systems efficiently in terms of the problems related to scalability and interoperability [37,48] (all respondents). Adding to the complexities are also the availability of multiple platforms, numerous protocols, large numbers of APIs and well evolving standards. *IoT environment constraints* to date present many security challenges in terms of devices computational power, memory, battery, network, operating system, and bandwidth, among others [19,22,43,52] (R1, R2, R6). *Constant evolution* of new IoT technologies, *heterogeneity and continuous updates* of technologies present challenges regarding potential security vulnerabilities [22,49] (R6). Furthermore, *business and technical level standards* must not be taken lightly as IoT security constraints [44]. *Fragmentation of IoT market* with incompatible devices, platforms and protocols impose further challenges in implementing effective security measures (R1, R2). *Multiple Verticals* systems as created by IoT stakeholders contribute to fragmentation and interoperability problems within the IoT industry creating standardization challenges (R2).

5. Towards Openness and Security Thinking Model for IoT Ecosystems

The complexity of IoT ecosystems has led us to present our results that show how openness and security thinking are important characteristics for such complex ecosystems. Figure 2 conceptualizes the above-mentioned openness and security characteristics obtained from the research results.

Figure 2 shows two major important aspects, the openness and security thinking which are represented by various design aspects. In the context of openness, the open architecture approach plays a significant role. This approach provides the means for establishing the design and development settings that capture the characteristics as attributes or constraints of a system in an open way [6]. Design principles of an open architecture approach can be put into view from two perspectives: (a) design and development, and (b) architectural design perspectives. The model presented in Figure 1 and re-purposed in Figure 2 can be used to identify and then tackle the needs related to building an open IoT system. Such a system has the ability to grow, mature and even change over time from a bottom-up perspective. The importance of the bottom-up perspective shows that, while changes are unavoidable, the open architecture approach can be applied during the design phase of the system and architecture that helps to establish the design and development settings. In these new settings, the open architecture characteristics and their properties can be enabled. An open architecture approach helps designers, developers, and domain experts to easily and flexibly integrate, customize, and extend the IoT products.

Our results, however, show that openness is not determined by aspects of flexibility, customizability and extensibility alone, further extended with open standards, open data, open APIs, open processes, open source for the IoT ecosystems, but are heavily dependent on security and privacy aspects too. For example, improper choice of openness leads to opening up larger attack surfaces. To illustrate this further, a software library may not be properly maintained and a software can by default be shipped with diverse features that may have not necessarily been tested against security and privacy threats. Therefore, in light of our proposal for a continuous security thinking approach, we argue that concepts and models towards conceptualizing security in IoT can be both innovative and risky at the same time, mainly due to their constricted singular view upon the IoT ecosystems. We thus identify new dimensions and a number of aspects that are important for continuous security thinking in IoT, targeting not only practitioners alone, but also developers, users and the society at large. Table 3 highlights our conceptual framework derived from the state-of-the-art and interviews that initiated the development of our three-dimensional model for continuous security thinking in relation to *awareness*, *assessment* and *challenges*. This table presents the mapping of three dimensions with a number of aspects identified that are important for IoT security thinking. In reference to our findings presented as three dimensions, the call to mitigate security risks almost two decades ago still remains vital today: "the open and semi-chaotic Internet. . . is the creation of opportunities for leakage of threats from robust into vulnerable networks" [26]. Our study shows that there is a need for continuous security thinking in terms of *awareness*, *assessment* and *challenges* that are new dimensions for security in IoT ecosystems.

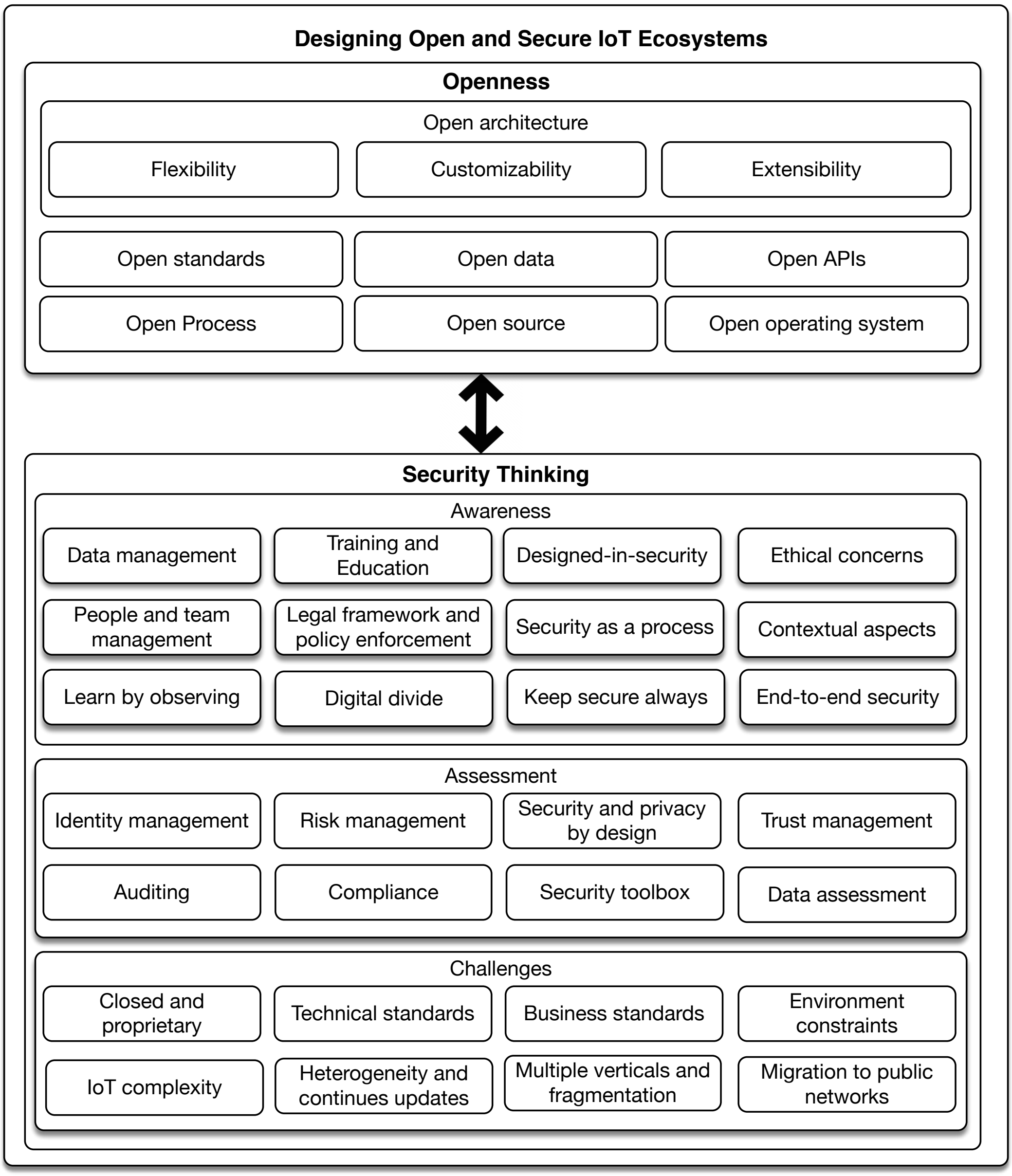

Figure 2. Open and Secure IoT design model conceptualized.

Aspects of awareness and assessment are critical since they represent a relationship to people, such as IoT development community, security practitioners and their involvement in the development life-cycle. Thus, they become specifically important in the initial design phase of the system. Awareness is about cultivating a security mindset among IoT practitioners, such as by providing appropriate security training. Security should be introduced in a form of security as a process aspect that would help thinking about security from the initial design phase and throughout the development lifecycle. Developers should better understand the context of operation and then apply security aspects that work for them, as often it is not possible to state the exact guidelines for designing secure IoT system. Assessment, on the other hand, should let IoT developers think about necessary tools and software assessment. For example, a security toolbox helps practitioners conduct e.g., threat modeling, architectural review, code review, and running automated security tests. Moreover, security risk assessment e.g., by incorporating threat modeling iteratively, system architecture reviews, and other related mechanisms as well as the need to frame security requirements on the system and platform by the practitioners. With trust management and data assessment developers need to manage and assess device trust, entity trust, data trust and include strong authenticity into the system in order to assess data for its correctness, trustworthiness, and reliability. In the process of implementing security thinking in IoT, one can encounter various challenges related to resource constraints, operational environment and heterogeneity [30]. Challenges related to resource constraints such as processing power, battery, memory, space, etc. that put restrictions on the type of security solutions can be used. Challenges related to operational environment in terms of complex, dynamic and distributed execution environment pose further issues on usage of existing security and privacy mechanisms.

Our conceptualized model emphasizes the human in the loop concept that would help to easily understand the emerging needs as design principles for IoT ecosystems in a more open and secure way. Furthermore, with these conceptualizations, people could actively take part and shape their IoT tools in a more transparent way. Thus, in general, we believe that openness leans toward more transparency when implementing security, e.g., Blockchain as a promising technology can be very beneficial for auditing data and fostering more guaranteed assurances that certain aspects of security and privacy are in check. For example, autonomous systems, from cars to pacemakers, can become serious malfunctioning systems led by weak security thinking. While such failures often become headlines in the press, they have yet to receive full attention by the IoT community to bring security thinking at the forefront. In this study, we show that novelty and risks concurrently target security in the IoT, and thus the importance of the three identified dimensions: awareness, assessment and challenges, together with a number of aspects, uplift continuous security thinking. With our findings, we make an attempt to reverse the mindset that security is not guaranteed in IoT systems, particularly that the three-dimensional model can help pave the way for a future robust and secure IoT system. It is often reported that the speed of IoT technology surpasses the capacity for the existing security requirements to keep the technological environment more secure. With continuous security thinking at hand, we foresee that an IoT security agenda can be built beforehand as a precursor to secure IoT technological developments.

To design an IoT system based on openness and security characteristics requires that their respective aspects are considered as presented above by the practitioners in the field. The importance of emphasising these aspects often refers to the benefits to be used proactively in the first phase when setting up a specific security design together with the set of grounding requirements as discussed above, and introduced in Figure 2 and Table 3. While the model does not show how each aspect is prioritized as presented in Figure 2, prioritization is not an obstacle for applying the proposed model in practice, particularly because the model must be adapted and applied according to the needs of respective organizations and their challenges.

Table 3. Three dimensions and related aspects for IoT Security Thinking .

Aspects	**Sources**
Continuous Awareness	
Data management	Aggarwal et al. [40]; Benson et al. [41]; Kolias et al. [42]
Training and education	Stallings et al. [45]; Törngren et al. [37]; Izosimov and Törngren [44]; Dhillon et al. [27]; Harbers et al. [48]; Bugeja et al. [43]; All respondents
Designed-in security	Peisert [46]; Miorandi [59], Bugeja et al. [43]
People and team management	Wan and Zeng [49]
Contextual aspects	All respondents
Learn by observing	R5
Legal framework and policy enforcement	Weber [14]; Hoepman [50]; Porras et al. [52]
Security as a process	Vogel and Varshney [19], Bugeja et al. [43]; R5
Addressing the digital divide	R1; R6
Keep secure always	All respondents
Plan for end-to-end security	R6; Bugeja et al. [43]
Ethical concerns	Kaleta et al. [47]; Dhillon et al. [27]
Continuous Assessment	
Identity management	Kounelis et al. [53]; Kumar et al. [54]; Dhillon et al. [27]; Sfar et al. [55]
Risk management	Izosimov and Törngren [44]; Choobineh et al. [56]; Peisert et al. [46]; Törngren et al. [37], Bugeja et al. [43]; R5, R6
Security and privacy by design principles	Hoepman [50] ; Harbers et al. [48], Bugeja et al. [43]; Cha et al. [57]; All respondents
Trust management	Sicari et al. [51]; Porras et al. [52]; Sfar et al. [55]; Vogel and Varshney [19]; R1; R2
Auditing	Dhillon et al. [27] ; Ali et al. [58]; R5; R6
Compliance	Kajtazi et al. [29]; Dhillon et al. [27]; Moody et al. [28]; Ali et al. [58], Bugeja et al. [43]
Security toolbox	Bugeja et al. [43], Vogel and Varshney [19]; R5
Data assessment	Bugeja et al. [43], Vogel and Varshney [19]; Cha et al. [57]; R1; R6
Continuous Challenges	
Closed and proprietary	Benson et al. [41]; Kolias et al. [42]; Vogel and Gkouskos[6];Bugeja et al. [43];
Standards (both technical and business level)	Kolias et al. [42]; Izosimov and Törngren [44], Bugeja et al. [43]; R2; R6
IoT complexity	Harbers et al. [48]; Törngren et al. [37]; Bugeja et al. [43]; All respondents
IoT environment (resource) constraints	Porras et al. [52] ; Agarwal and Dey [22]; Vogel and Varshney [19]; R1; R2; R6
Heterogeneity and continuous updates	Wan and Zeng [49]; Agarwal and Dey [22], Vogel and Varshney [19]; R6
Multiple verticals and Fragmentation	R1; R2
Migration to public networks	R5

6. Study Limitations

Various limitations were encountered during the research phase. The literature study is not comprehensive, but it takes into account recent developments connected to IoT openness and security. Moreover, IoT practitioners and security experts insights complement the retrieved literature. In addition, we tried to minimize the bias by the interview method as the idea was to validate the results obtained from state-of-the-art. Interviews were conducted with the total of six subjects, which might pose some threats to the results. It is worth mentioning that a pilot interview was conducted with one of the respondents to validate the design guide of the interviews. With the intention to minimize bias, subjects of this study were selected from a wide range of organizations such as from start-ups to big players in the IoT industry. Moreover, for the purpose of validity aspects of this research, study subjects were selected based on different roles, i.e., security architects, senior architect, technology experts, technology leader, security coach, security expert.

7. Conclusions and Future Perspectives

The goal of this paper was to prioritize openness and security thinking as mandatory characteristics for the IoT ecosystems. We proposed the state-of-the-art and provided empirical input by understanding how practitioners view openness and security for IoT ecosystems. In general, we consider that there is a need for orchestrating smart services and devices in a more open, common and secure way that affect the dynamic operating conditions of IoT environments. We therefore proposed a set of openness and security thinking characteristics as a basis to address some of the persistent challenges in the IoT field. With such characteristics considered thoroughly, the IoT system can meet its present and future requirements. Putting these characteristics in the right action, we consider that their power can help govern and make the IoT systems more open and at the same time more secure.

Reflecting upon our overall study, we consider that security is hard to be achieved specifically in the field of IoT. This is mainly due to constantly evolving new technologies and platforms that create extreme heterogeneity and fragmentation due to a lack of standardization. The results show that there is a need for a higher level of openness between different IoT systems to address the fragmentation and interoperability challenges. Openness is about using open standards, data, APIs, processes, source and open architectures (flexibility, customizability and extensibility), which provides direct benefits for IoT ecosystems such as easiness, convenience and fast development resulting in major cost-savings. We are of the thought that organizations should not rely exclusively on closed systems including algorithms, AI and ML for attaining security and privacy. Such systems can be reverse engineered exposing sensitive information and potentially very confidential information about the company, its employees and customers, and its processes. Thus, the dynamic nature of IoT brings a need to have openness and new security thinking into this area. In terms of describing security thinking, the results of our study show that when it comes to secure IoT development there is a need for continuous security thinking in terms of awareness, assessment and challenges, more so than the development of a traditional application. As a result, we believe that openness characteristics are an inseparable part of security and vice versa when thinking about designing an open and secure IoT system. Increased awareness for security aspects is crucial for IoT developers and end-users to help reduce security risks. The best way to keep security on different stakeholders' attention is to offer continuous security awareness, training and education programs. Practitioners of IoT products and services should have designed with security concepts in mind. For raising awareness, there is a need to continuously think about several more aspects, particularly for data management, team management, legal frameworks, policy enforcement and ethical concerns. Next, assessment becomes key where practitioners always need to have in mind identity management, risk management, trust management, certifications and last but not least the compliance aspects. Assessment is useful as a mechanism for evaluating the effectiveness of security controls. Finally, challenges inform us that the IoT itself is a new environment, but with continuous challenges that often forego rules on how technology should be handled. Continuous challenges such as resource constraints and heterogeneity of devices, protocols and standards add to the difficulty of securing the IoT infrastructure.

The results of this study anchor an important, yet an often overlooked IoT technological development at a crucial phase: openness vs. security thinking. Focusing attention on how to design more open and secure IoT technological systems can push future studies to develop specific measures to objectively test how security thinking can turn into action for open IoT systems. Future research can also attempt to measure the impact continuous security thinking has on actual open IoT system by observing the activities performed by the users. Moreover, the idea is to validate the conceptual model to understand how acceptable this model is in different domains (e.g., smart health or smart home context). We also plan to extend the model with additional layers for each component to practically better emphasize the application of the model in certain scenarios. With IoT systems being the target of various security attacks, our study contributes to guiding IoT practitioners with secure habits when developing open IoT systems.

Author Contributions: Conceptualization, B.V. and M.K.; data curation, J.B. and R.V.; investigation, B.V. and M.K.; methodology, B.V., M.K. and R.V.; project administration, B.V.; writing—original draft, B.V. and M.K.; writing—review & editing, B.V., M.K., J.B. and R.V. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Stiftelsen för Kunskaps- och Kompetensutveckling Grant No. 20140035.

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

References

1. Markit, I. The Internet of Things: A Movement, Not a Market. IHS Markit, 2017. Available online: https://cdn.ihs.com/www/pdf/IoT_ebook.pdf (accessed on 1 December 2020).
2. Markit, I. The top trends of 2019: Powered by Transformative Technologies. IHS Markit, 2019. Available online: https://cdn.ihs.com/www/pdf/0119/IHS-Markit-2019-Trends-Report.pdf (accessed on 1 December 2020).
3. Columbus, L. 2018 Roundup Of Internet Of Things Forecasts In addition, Market Estimates. *Forbes* 13 December 2018.
4. Zuboff, S. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, 1st ed.; PublicAffairs: New York, NY, USA, 2019.
5. Bröring, A.; Schmid, S.; Schindhelm, C.K.; Khelil, A.; Käbisch, S.; Kramer, D.; Le Phuoc, D.; Mitic, J.; Anicic, D.; Teniente, E. Enabling IoT ecosystems through platform interoperability. *IEEE Softw.* **2017**, *34*, 54–61. [CrossRef]
6. Vogel, B.; Gkouskos, D. An open architecture approach: Towards common design principles for an IoT architecture. In Proceedings of the 11th European Conference on Software Architecture: Companion Proceedings, Canterbury, UK, 11–15 September 2017; pp. 85–88. [CrossRef]
7. Nikayin, F.; De Reuver, M. Governance of smart living service platforms: State-ofthe-art and the need for collective action. In Proceedings of the 3rd International Engineering Systems Symposium, Delft, The Netherlands, 18–20 June 2012.
8. Samsung. The Internet of Things needs openness and industry collaboration to succeed. *Samsung*, 27 October 2015.
9. Schlagwein, D.; Conboy, K.; Feller, J.; Leimeister, J.M.; Morgan, L. "Openness" with and without Information Technology: A framework and a brief history. *J. Inf. Technol.* **2017**, *32*, 297–305. [CrossRef]
10. Vogel, B.; Dong, Y.; Emruli, B.; Davidsson, P.; Spalazzese, R. What Is an Open IoT Platform? Insights from a Systematic Mapping Study. *Future Internet* **2020**, *12*, 73. [CrossRef]
11. Wickström, J.; Westerlund, M.; Pulkkis, G. Rethinking IoT Security: A Protocol Based on Blockchain Smart Contracts for Secure and Automated IoT Deployments. *arXiv* **2020**, arXiv:cs.CR/2007.02652.
12. Alaba, F.A.; Othman, M.; Hashem, I.A.T.; Alotaibi, F. Internet of Things Security. *J. Netw. Comput. Appl.* **2017**, *88*, 10–28. [CrossRef]
13. Wu, H.; Han, H.; Wang, X.; Sun, S. Research on Artificial Intelligence Enhancing Internet of Things Security: A Survey. *IEEE Access* **2020**, *8*, 153826–153848. [CrossRef]

14. Weber, R.H. Internet of things: New security and privacy challenges. *Comput. Law Secur. Rev.* **2010**, *26*, 23–30. [CrossRef]
15. Konstantina, S.; Zeynep, G.; Catherine, M.E.L. Organizational cloud security and control: A proactive approach. *Inf. Technol. People* **2019**. [CrossRef]
16. Mansfield-Devine, S. *Open Source and the Internet of Things*; Network Security; Elsevier: Amsterdam, The Netherlands, 2018; pp. 14–19.
17. Lowry, P.B.; Dinev, T.; Willison, R. Why security and privacy research lies at the centre of the information systems (IS) artefact: Proposing a bold research agenda. *Eur. J. Inf. Syst.* **2017**, *26*, 546–563. [CrossRef]
18. McDermott, C.D.; Isaacs, J.P.; Petrovski, A.V. Evaluating Awareness and Perception of Botnet Activity within Consumer Internet-of-Things (IoT) Networks. *Informatics* **2019**, *6*, 8. [CrossRef]
19. Vogel, B.; Varshney, R. Towards Designing Open and Secure IoT Systems: Insights for Practitioners. In Proceedings of the 8th International Conference on the Internet of Things, Santa Barbara, CA, USA, 15–18 October 2018; ACM: New York, NY, USA, 2018; pp. 36:1–36:6. [CrossRef]
20. Kajtazi, M.; Vogel, B.; Bugeja, J.; Varshney, R. State-of-the-Art in Security Thinking for the Internet of Things (IoT). In Proceedings of the 13th Pre-ICIS Workshop on Information Security and Privacy, San Francisco, CA, USA, 13 December 2018; Volume 5.
21. Weiser, M. The computer for the 21 stcentury. *Sci. Am.* **1991**, *265*, 94–104. [CrossRef]
22. Agarwal, Y.; Dey, A.K. Toward Building a Safe, Secure, and Easy-to-Use Internet of Things Infrastructure. *Computer* **2016**, *49*, 88–91. [CrossRef]
23. Caporuscio, M.; Ghezzi, C. Engineering Future Internet applications: The Prime approach. *J. Syst. Softw.* **2015**, *106*, 9–27. [CrossRef]
24. Vogel, B. Towards Open Architecture System. In Proceedings of the 2013 9th Joint Meeting on Foundations of Software Engineering, ESEC/FSE 2013, Saint Petersburg, Russia, August 18–26 2013; ACM: New York, NY, USA, 2013; pp. 731–734. [CrossRef]
25. Vogel, B.; Kurti, A.; Mikkonen, T.; Milrad, M. Towards an Open Architecture Model for Web and Mobile Software: Characteristics and Validity Properties. In Proceedings of the 2014 IEEE 38th Annual Computer Software and Applications Conference, Vasteras, Sweden, 21–25 July 2014; pp. 476–485. [CrossRef]
26. Sicker, D.C.; Lookabaugh, T. VoIP Security: Not an Afterthought. *Queue* **2004**, *2*, 56–64. [CrossRef]
27. Dhillon, G.; Carter, L.; Abed, J.; Sandhu, R. Defining Objectives For Securing The Internet of Things: A Value-Focused Thinking Approach. *WISP Proc.* **2016**, *3*.
28. Moody, G.; Siponen, M.T.; Pahnila, S. Toward a Unified Model of Information Security Policy Compliance. *MIS Q.* **2018**, *42*, 285. [CrossRef]
29. Kajtazi, M.; Cavusoglu, H.; Benbasat, I.; Haftor, D. Escalation of commitment as an antecedent to noncompliance with information security policy. *Inf. Comput. Secur.* **2018**, *26*, 171–193. [CrossRef]
30. Varshney, R. Towards Designing Open Secure IoT System—Insights for Practitioners. Master's Thesis, Malmo University, Malmo, Sweden, 2018.
31. Atzori, L.; Iera, A.; Morabito, G. Understanding the Internet of Things: Definition, potentials, and societal role of a fast evolving paradigm. *Ad Hoc Netw.* **2017**, *56*, 122–140. [CrossRef]
32. Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M. Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. *Future Gener. Comput. Syst.* **2013**, *29*, 1645–1660. [CrossRef]
33. Preventis, A.; Stravoskoufos, K.; Sotiriadis, S.; Petrakis, E.G.M. IoT-A and FIWARE: Bridging the Barriers Between the Cloud and IoT Systems Design and Implementation. In Proceedings of the 6th International Conference on Cloud Computing and Services Science, CLOSER 2016, Rome, Italy, 23–25 April 2016; SCITEPRESS—Science and Technology Publications, Lda: Setubal, Portugal, 2016; Volume 1–2, pp. 146–153. [CrossRef]
34. Aly, M.; Khomh, F.; Guéhéneuc, Y.; Washizaki, H.; Yacout, S. Is Fragmentation a Threat to the Success of the Internet of Things? *IEEE Internet Things J.* **2019**, *6*, 472–487. [CrossRef]
35. Petersen, H.; Baccelli, E.; Wählisch, M. Interoperable Services on Constrained Devices in the Internet of Things. 2014. Available online: https://www.w3.org/2014/02/wot/papers/baccelli.pdf (accessed on 1 December 2020).
36. Riahi, A.; Natalizio, E.; Challal, Y.; Mitton, N.; Iera, A. A systemic and cognitive approach for IoT security. In Proceedings of the 2014 International Conference on Computing, Networking and Communications (ICNC), Honolulu, HI, USA, 3–6 February 2014; pp. 183–188. [CrossRef]

37. Törngren, M.; Bensalem, S.; McDermid, J.; Passerone, R.; Sangiovanni-Vincentelli, A.; Schätz, B. Education and Training Challenges in the Era of Cyber-Physical Systems: Beyond Traditional Engineering. In Proceedings of the WESE'15: Workshop on Embedded and Cyber-Physical Systems Education, Amsterdam, The Netherlands, 4–9 October 2015; ACM: New York, NY, USA, 2015; pp. 8:1–8:5. [CrossRef]
38. Dhillon, G.; Backhouse, J. Current directions in IS security research: Towards socio-organizational perspectives. *Inf. Syst. J.* **2001**, *11*, 127–154. [CrossRef]
39. Simmonds, A.J.; Sandilands, P.; van Ekert, L. *An Ontology for Network Security Attacks*; AACC; Springer: Berlin/Heidelberg, Germany, 2004.
40. Aggarwal, C.C.; Ashish, N.; Sheth, A. The Internet of Things: A Survey from the Data-Centric Perspective. In *Managing and Mining Sensor Data*; Aggarwal, C.C., Ed.; Springer: Boston, MA, USA, 2013; pp. 383–428. [CrossRef]
41. Benson, K.; Fracchia, C.; Wang, G.; Zhu, Q.; Almomen, S.; Cohn, J.; D'arcy, L.; Hoffman, D.; Makai, M.; Stamatakis, J.; et al. SCALE: Safe community awareness and alerting leveraging the internet of things. *IEEE Commun. Mag.* **2015**, *53*, 27–34. [CrossRef]
42. Kolias, C.; Stavrou, A.; Voas, J.; Bojanova, I.; Kuhn, R. Learning Internet-of-Things Security "Hands-On". *IEEE Secur. Priv.* **2016**, *14*, 37–46. [CrossRef]
43. 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. [CrossRef]
44. Izosimov, V.; Törngren, M. Security Evaluation of Cyber-Physical Systems in Society- Critical Internet of Things. In Proceedings of the TRUDEVICE—6th Conference on Trustworthy Manufacturing and Utilization of Secure Devices, Barcelona, Spain, 14–16 November 2016.
45. Stallings, W.; Brown, L. *Computer Security: Principles and Practice*, 3rd ed.; Pearson: Hoboken, NJ, USA, 2015.
46. Peisert, S.; Margulies, J.; Nicol, D.M.; Khurana, H.; Sawall, C. Designed-in Security for Cyber-Physical Systems. *IEEE Secur. Priv.* **2014**, *12*, 9–12. [CrossRef]
47. Kaleta, J.; Thackston, R.; Ojagbule, O. Exploring User Privacy Based on Human Behavior with Internet of Things Devices at Home (Formative Research). *SAIS 2018 Proc.* **2018**, *6*. Available online: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1021&context=sais2018 (accessed on 1 December 2020).
48. Harbers, M.; Bargh, M.S.; Pool, R.; Berkel, J.V.; van den Braak, S.W.; Choenni, S. *A Conceptual Framework for Addressing IoT Threats: Challenges in Meeting Challenges*; HICSS: Hilton Waikoloa Village, HI, USA, 2018.
49. Wan, J.; Zeng, M. Research on Key Success Factors Model for Innovation Application of Internet of Things with Grounded Theory. *WHICEB 2015 Proc.* **2015**, *38*.
50. Hoepman, J.H. Privacy Design Strategies. In *ICT Systems Security and Privacy Protection*; Cuppens-Boulahia, N., Cuppens, F., Jajodia, S., Abou El Kalam, A., Sans, T., Eds.; Springer: Berlin/Heidelberg, Germany, 2014; pp. 446–459.
51. Sicaria, S.; Rizzardia, A.; Griecob, L.A.; Coen-porisinia, A. Security, privacy and trust in Internet of Things: The road ahead. *Comput. Netw.* **2015**, *76*, 146–164. [CrossRef]
52. Porras, J.; Pänkäläinen, J.; Knutas, A.; Khakurel, J. *Security In The Internet Of Things—A Systematic Mapping Study*; HICSS: Hilton Waikoloa Village, HI, USA, 2018.
53. Kounelis, I.; Baldini, G.; Neisse, R.; Steri, G.; Tallacchini, M.; Guimaraes Pereira, A. Building Trust in the Human? Internet of Things Relationship. *IEEE Technol. Soc. Mag.* **2014**, *33*, 73–80. [CrossRef]
54. Kumar, S.A.; Vealey, T.; Srivastava, H. Security in Internet of Things: Challenges, Solutions and Future Directions. In Proceedings of the 2016 49th Hawaii International Conference on System Sciences (HICSS), Koloa, HI, USA, 5–8 January 2016; pp. 5772–5781.
55. Sfar, A.R.; Natalizio, E.; Challal, Y.; Chtourou, Z. A roadmap for security challenges in the Internet of Things. *Digit. Commun. Netw.* **2018**, *4*, 118–137. [CrossRef]
56. Choobineh, J.; Dhillon, G.; Grimaila, M.R.; Ulmer, J.R. Management of Information Security: Challenges and Research Directions. *Commun. Assoc. Inf. Syst.* **2007**, *20*, 57. [CrossRef]
57. Cha, S.; Hsu, T.; Xiang, Y.; Yeh, K. Privacy Enhancing Technologies in the Internet of Things: Perspectives and Challenges. *IEEE Internet Things J.* **2019**, *6*, 2159–2187. [CrossRef]
58. Ali, I.; Sabir, S.; Ullah, Z. Internet of Things Security, Device Authentication and Access Control: A Review. *arXiv* **2019**, arXiv:abs/1901.07309.

59. Miorandi, D.; Sicari, S.; Pellegrini, F.D.; Chlamtac, I. Internet of things: Vision, applications and research challenges. *Ad Hoc Netw.* **2012**, *10*, 1497–1516. [CrossRef]

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.