future internet

Article

What Is an Open IoT Platform? Insights from a Systematic Mapping Study

Bahtijar Vogel [1,2,*], Yuji Dong [1,2,*], Blerim Emruli [1,2,3], Paul Davidsson [1,2] and Romina Spalazzese [1,2]

[1] Department of Computer Science and Media Technology, Malmö University, 20506 Malmö, Sweden; blerim.emruli@ics.lu.se (B.E.); paul.davidsson@mau.se (P.D.); romina.spalazzese@mau.se (R.S.)
[2] Internet of Things and People Research Center, Malmö University, 20506 Malmö, Sweden
[3] Department of Informatics, Lund University, 22363 Lund, Sweden
* Correspondence: bahtijar.vogel@mau.se (B.V.); yuji.dong@mau.se (Y.D.)

Received: 3 March 2020; Accepted: 15 April 2020; Published: 18 April 2020

Abstract: Today, the Internet of Things (IoT) is mainly associated with vertically integrated systems that often are closed and fragmented in their applicability. To build a better IoT ecosystem, the open IoT platform has become a popular term in the recent years. However, this term is usually used in an intuitive way without clarifying the openness aspects of the platforms. The goal of this paper is to characterize the openness types of IoT platforms and investigate what makes them open. We conducted a systematic mapping study by retrieving data from 718 papers. As a result of applying the inclusion and exclusion criteria, 221 papers were selected for review. We discovered 46 IoT platforms that have been characterized as open, whereas 25 platforms are referred as open by some studies rather than the platforms themselves. We found that the most widely accepted and used open IoT platforms are NodeMCU and ThingSpeak that together hold a share of more than 70% of the declared open IoT platforms in the selected papers. The openness of an IoT platform is interpreted into different openness types. Our study results show that the most common openness type encountered in open IoT platforms is open-source, but also open standards, open APIs, open data and open layers are used in the literature. Finally, we propose a new perspective on how to define openness in the context of IoT platforms by providing several insights from the different stakeholder viewpoints.

Keywords: internet of things; IoT; open IoT platforms; openness; open-source; open standards; open API; systematic mapping study

1. Introduction and Motivation

After decades of development, the Internet of Things (IoT) has evolved into a fully fledged ecosystem including hardware, software, physical objects and people with complex interactions and data exchanges. The number of users, services and applications with IoT is rapidly growing in many different domains [1]. The development of new intelligent applications can benefit from IoT in almost every field from personal everyday life to environment and society. Borgia [2] classifies the various IoT applications into three major domains—industrial domain, smart city domain and health well-being domain—and gives many related applications as examples such as farm management [3], smart grid [4], and remote healthcare [5]. Because of the huge potentialities in IoT, the demands for new services and applications are massive.

The IoT market is predicted to grow, by some estimates, from 50 billion [6] to 100 billion [7] devices by 2020. Other more modest projections state that there will be 24 billion [1] and 26 billion [8] devices by the same year. The large number of devices builds a solid foundation as the device layer. Numerous services and applications can be further developed based on devices with many different technologies [9]. However, such a scale of devices and various enabling technologies make the development of IoT systems complicated and difficult. For these issues, IoT platforms play a significant role in helping the integration and development of IoT systems.

As a result, new IoT platforms are constantly emerging, which forms a new layer in Cyber-Physical Systems (CPSs) [10]. These IoT platforms already offer heterogeneous ways to access them and their data [11]. According to the Minerauda et al. [12] an "IoT platform is defined as the middleware and the infrastructure that enables the end users to interact with smart objects". There are different types of platforms available that often are referred to as IoT platforms, such as device-to-device, cloud-based and device-to-cloud platforms (which are often also referred to as enterprise platforms that face a vendor lockdown [13–15]). The diversity of IoT platforms and their complex offerings creates confusion among developers and researchers, as well as end users. As such, today the IoT is mainly associated with vertically integrated systems that often are closed and fragmented in their applicability. For example, there are multiple IoT platforms, which partially comply with standards; diverse mobile platforms and systems, where the operating systems and programming languages are different; and physical devices that have varying characteristics [11,16]. With such closed nature and fragmentation in the market, developers usually struggle to reach critical mass, and even end users need to navigate through different brands and understand which devices are compatible in relation to which IoT platforms. Commercial or proprietary IoT platforms carry a pricing model and often promote vendor lock-in. Thus, often IoT platform providers lack support of new protocols, tools and data formats in time due to a constantly changing IoT landscape. Openness, on the other hand, is one of the emerging trends that is evident in IoT domains [16–18]. More and more IoT players are motivated to use open systems due to the associated benefits such as convenience and fast development resulting in major cost savings for the industry [17,19]. From a general perspective, innovation, entrepreneurship, creativity and new business models also require openness to build a valuable ecosystem based on our previous experience in the Internet economy [20].

Several interesting studies provide analysis of some open and closed IoT platforms [12,21–24]. A study on gap analysis of IoT platforms lists a representative sample of both open and closed ones, providing an overview of actual platforms, their heterogeneity, type, deployment architectures, availability and data access [12]. Another study focuses in surveying IoT platforms for massive sensing and actuation, and discusses some of the platforms and mainly ideas about how they work, including strengths and weaknesses [25]. A survey of IoT cloud platforms is also provided [21], while identifying suitable middleware platforms to manage things and applications with a reliable solution [22]. In two other studies, three open-source platforms and one proprietary are compared while discussing concepts, similarities and differences [23,24]. Despite several efforts contributing to open platforms having been done, there is no consensus about what characterizes an open IoT platform.

To the best of our knowledge, no comprehensive study on research related to open IoT platforms exists addressing what makes them "open". Thus, the goal of our study is to characterize open IoT platforms by using a Systematic Mapping Study, and to gain new knowledge of what makes the IoT platform open.

Below we highlight the contributions of our study:

1. We provide a comprehensive overview of the "open IoT platforms" to the research community via a systematic mapping study. Openness as trend has significantly increased during recent years. One factor of this trend is the emerging interest of research in the use of openness in the IoT domain.
2. We identified 46 IoT platforms as "used", "indicated" and "proposed" from 221 analyzed papers. We highlighted the seven most used open IoT platforms. We note that NodeMCU and ThingSpeak are widely adopted platforms among the research community with the biggest share, followed by FIWARE, Mobius, Kaa, OpenIoT, and ThingsBoard.

3. We map all the identified open IoT platforms into six openness types: *open-source*, *open standards*, *open APIs*, *open data*, *open layer* and *not specified* with emphasis to understand why the IoT platforms are known as "open". We also note that some papers express the same open IoT platform with different openness types, while the most dominant openness type labeled among the analyzed studies is "open-source".
4. Finally, we propose a new perspective on how to define openness in the context of IoT platforms by providing several insights from the different stakeholder viewpoints, which interprets the differences among all the papers' different expressions of the openness of IoT platforms.

The rest of the paper is organized as follows. In Section 2, we discuss our research method. We present the obtained results and analysis from the selected studies in Section 3. Thereafter, we discuss the results of our review (Section 4), followed by some limitations highlights (Section 5) and finally we conclude the study (Section 6).

2. Research Method

In our study, we use a systematic mapping study which consists of planning, conducting and reporting as proposed by Petersen et al. [26]. During the planning phase, all decisions for conducting the mapping study are made, such as defining the scope and research questions. Review protocol is established by the team, which describes the procedure to conduct the study [26]. In the conducting phase, first, studies were selected and then data was extracted and analyzed. This phase was iterative [26]. In the reporting phase, the study results were summarized and reported [26]. The most important part of systematic studies is the planning phase of the review protocol to ensure rigor and reproducibility of the study [27]. In our review protocol, we identified the research questions and a search string, then we used the manual search in our strategy that led us to define the search scope. During this step we performed pilot searches then we developed inclusion and exclusion criteria. The pilot searches helped us to refine both the search strings and the criteria. Finally, relevant publishers in the IoT field are used as data sources.

2.1. Research Questions

The goal of this study is to characterize open IoT platforms from the researcher point of view. We use a Goal–Question–Metric (GQM) approach to classify our goal with aspects of purpose, issue, object and viewpoint [28]:

- `purpose`: characterize
- `issue`: openness in
- `object`: open IoT Platforms
- `viewpoint`: from the researcher point of view

The main goal of this mapping study is refined into two research questions:

- **RQ1:** What IoT platforms have been characterized as open?
- **RQ2:** Which are the openness types of open IoT platforms?

With RQ1 we aim to provide a general overview of the state of the art of IoT platforms that have been used and indicated to be *open IoT platforms*. With RQ2 we are interested to identify the openness types of IoT platforms and gain new knowledge of what makes the open IoT platform.

2.2. Search Strategy and Sources

The search strategy is composed of different steps. At first, we performed some trial searches in IEEE and ACM digital libraries by trying and testing different search strings in relation to RQs. However, to get more accurate results, we decided to use Google Scholar as it was better to query and filter our data. After some additional trial searches, we defined the following search string:

*"open * IoT * Platform" OR "open IoT * Platform" OR "open * IoT Platform" OR "open IoT Platform" OR "open * Internet of Things * Platform" OR "open Internet of Things * Platform" OR "open * Internet of Things Platform" OR "open Internet of Things Platform"*

We used Publish or Perish [29] to easily retrieve the data from Google Scholar and have them in a format suited for analysis. Based on the above search string, we retrieved the data until our last conducted search on 30 September 2019 that included 718 papers. However, we note that based on our search string the earliest published papers related to open IoT platforms start from 2012.

2.3. Inclusion and Exclusion Criteria

Inclusion and exclusion criteria helped our team to identify and classify the studies based on our research questions. The papers were selected if they strictly met any inclusion criteria and thus were classified, and were excluded if it met any exclusion criteria. The following inclusion criteria were applied:

1. Studies that propose a new open IoT platform
2. Studies that use an existing open IoT platform
3. Studies that use, define or indicate the term "open" with respect to IoT platforms
4. Studies that are part of well-known sources and databases related to publications as listed below

The following exclusion criteria were applied:

1. Tutorials, BSc/MSc thesis, editorials, opinions, abstracts only, because they might not contain sufficient data for our study.
2. Studies not written in English
3. Open IoT platform mentioned only in references

For inclusion criteria 4, we limited our search scope to the sources and databases that are well-known in the IoT field related to publications:

- IEEE Explore,
- ACM Digital Library,
- SpringerLink,
- ScienceDirect, and
- Wiley.

One of the main reasons for choosing these sources and databases was based on the suggestions of Brereton et al., [30] and Dyba at el., [31] to perform more exhaustive searches in our field of study. Having in mind that IoT publication venues are still developing, additionally we used other sources as well:

- MDPI,
- Emerald Group Publishing,
- IET, and
- SAGE Publications.

After applying the above limitation based on publications and language where we started to apply the inclusion and exclusion criteria, we obtained 353 papers that we then downloaded and analyzed them (see downloaded studies (http://doi.org/10.5281/zenodo.3755257)).

2.4. Search Process and Data Extraction

Figure 1 shows our search process where we used initial and trial searches (1.1) to identify the topic relevancy, and to define the final search for stage 1.2 query. Further on, inclusion and exclusion criteria (stage 2) are continuously applied which led us to the final review and analysis at Stage 3. The data is collected and classified based on studies that: "use", "propose", "define", "indicate" or studies with "no explanation" in relation to open IoT platforms, explained below:

- With the *use* category we mean the papers that have used at least one open IoT platform in their implementation, deployment or testing.
- By *indicate*, we mean the papers that point out the open IoT platform, independent of their implementation or testing.
- Papers categorized under *propose* explicitly deal with the newly suggested open IoT platforms.
- By *define*, we mean the papers that attempt to provide a definition of the openness aspects of platforms.
- By the studies with "no explanation" we mean the papers that use the term open IoT platform but with no further explanation, e.g., the term used in introduction, background, related work or anywhere including the conclusions within this category of studies.

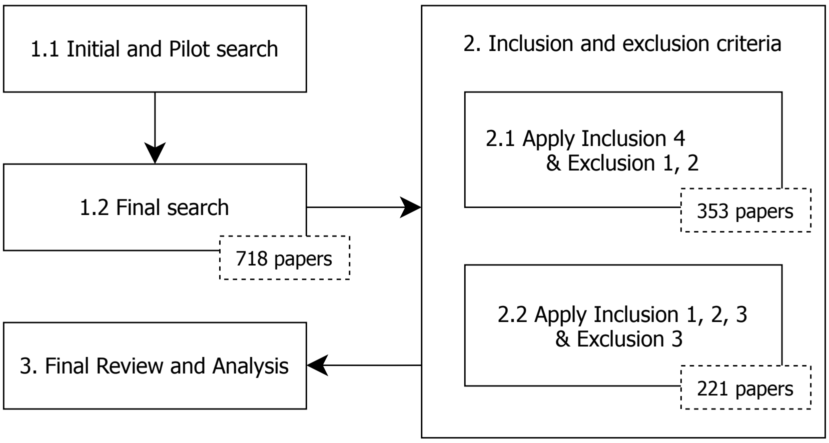
1.1 Initial and Pilot search
1.2 Final search
718 papers
3. Final Review and Analysis
2. Inclusion and exclusion criteria
2.1 Apply Inclusion 4 & Exclusion 1, 2
353 papers
2.2 Apply Inclusion 1, 2, 3 & Exclusion 3
221 papers

Figure 1. Search Process.

Three researchers in parallel were involved in this process. During the process, the researchers discussed their findings and viewpoints with two additional researchers for validity purposes of the overall study. Moreover, all five researchers met regularly. To minimize the threats of our study, during the classification and mapping process ambiguity was addressed among the team, e.g., the challenges a researcher faced when mapping some studies in defined categories. During these meetings, all disagreements were discussed and resolved. In Table 1, we enlist the data extraction items and their relations with RQs.

Table 1. Data extraction items.

-	Field	RQs
F1	Author(s)	na
F2	Year	na
F3	Title	na
F4	Abstract	na
F5	Publisher	na
F6	Venue	na
F7	Open IoT platforms in "use"	RQ1, RQ2
F8	Open IoT platforms "indicated"	RQ1, RQ2
F9	Open IoT platforms "defined"	RQ2
F10	Open IoT platforms "proposed"	RQ2
F11	Openness type in "use", "indicated" and "proposed" Platforms	RQ2
F12	Open IoT platforms with "no explanation"	RQ2

The data is stored in online spreadsheets (to ease the collaboration and ensure reproducibility of the study) and was manually reviewed. Mainly qualitative data is collected but also some quantitative such as number of citations, published year, published venue in order to derive some basic descriptive statistics that can be used to address the RQs or other intermediate hypotheses that arose during the process.

3. Results

As stated in Section 2.2, after we extracted data for 718 papers, we decided to limit our search scope to well-known publishers, which led us to download and analyze 353 papers. Moreover, after applying the inclusion and exclusion criteria (see Section 2.3), 221 papers were selected for the final review. We want to highlight that 59 papers categorized under *no explanation* are not included for the final review, as these papers did not provide any insights related to our study aim. Below, first we present the distribution of papers and some demographic data, and based on comparative analysis we address the research questions stated in Section 2.1.

3.1. Distribution of Papers

In the final review, as introduced above, we decided to classify and map the papers into five categories, i.e., *use, indicate, propose, define* and *no explanation* (for details about categorized papers see (http://doi.org/10.5281/zenodo.3755257)). The result of the classification process is presented below, such that:

- `use`: 134 papers,
- `indicate`: 56 papers,
- `propose`: 28 papers,
- `define`: 3 papers, and
- `no explanation`: 59 papers.

It is interesting to note that majority of the papers make use of open IoT platforms, plenty indicate or provide no explanation, and only three papers make an attempt to define what an open IoT platform is. In particular, we noted the large number of papers that mention open IoT platforms term but they *do not* provide explanation or give deeper insight; often by making use of the term superficially within the introduction, related work or future work sections. Driven by this finding, we decided to further analyze and quantify the distribution of the published articles with no explanation, which is presented in Figure 2. Among other things in Figure 2, we noted the *openness trend* that relates to open IoT platforms and that has significantly increased between 2016 and 2019 by number of published articles that *do not* provide explanation. As a comparison, Figure 2 also shows the total yearly publication distribution of the selected 221 articles. It is obvious to see the *openness trend* between the same years, 2016–2019.

Figure 2 shows an increasing trend for publishing open IoT platform-related papers. One factor of this trend, we believe, is the emerging interest of research in the use of openness in the IoT domain in recent years. These findings, to an extent, correlate well with the report of IoT analytics that is one of the leading providers for providing market insights and strategic business analytics for Industry 4.0 and IoT, stating that 450 companies created their IoT platforms in 2017, which is 25% more than in 2016, and that there is a tendency for this trend to increase even more over the coming years.

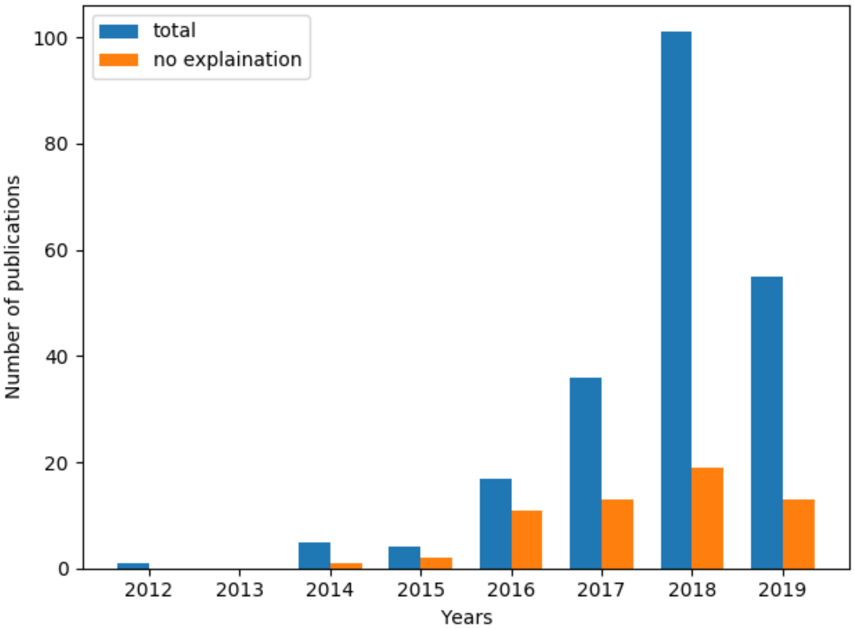

Figure 2. Distribution of the yearly publications related to open IoT platforms and articles with no explanation about open IoT platforms.

3.2. Q1: What IoT Platforms Have Been Characterized as Open?

To address this question we analyzed the data extracted from F7 and F8 stated in Table 1, i.e., open IoT platforms in "use" and "indicated". Table 2 reveals that there are 25 IoT platforms characterized as open by the studies. We note that there are seven open IoT platforms that are mainly used within the research community, whereas the other platforms are used only once or twice. For example, Figure 3 shows that most used open IoT platforms are NodeMCU and ThingSpeak, which together held a share of more than 70%, and are followed by FIWARE, Mobius, Kaa, OpenIoT, and ThingsBoard.

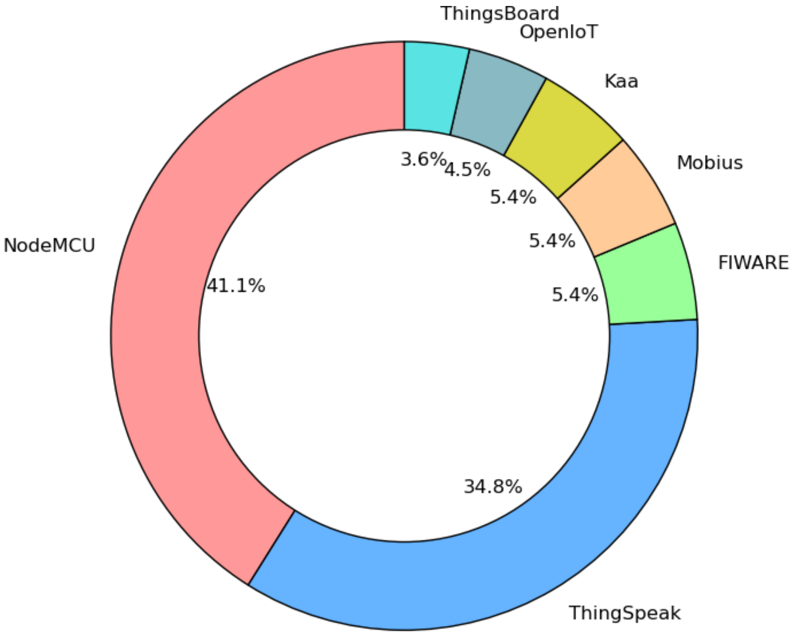

Figure 3. IoT platforms characterized as open based on studies that were classified as "use", totaling to 134 papers.

Table 2. The open IoT platforms identified in categories "used" and "indicated" in connection to the identified openness types.

#	Used/Indicated Platforms	Open-Source	Open Standards	Open APIs	Open Data	Not Specified
1	NodeMCU	45	1			1
2	ThingSpeak	29	1	4	2	12
3	OpenIoT	13	1	4	2	1
4	FIWARE	13	2	3	1	
5	KAA	9		5		
6	Mobius	6		3		
7	ThingsBoard	6		1	1	
8	IoTivity	3	1			
9	Oliot	2	1			
10	OM2M	2				
11	Arduino Raspberry Pi	1				1
12	Arduino Uno ESP8266	1				
13	Mobius			1		
14	Contiki OS	1				
15	Cosm OS	1		1		
16	Emon	1				
17	MediaSense	1				
18	RIOT	1				
19	Tacit					1
20	Heroku	1				
21	FLIP	1				
22	IoTMakers			1		
23	Tridium					1
24	VITAL-OS	1				
25	Californium	1				

Moreover, there is an interesting correlation between the referred open IoT platforms when they are "use" versus "indicated" by the researchers and practitioners, which is presented in Figure 4. In particular, we noticed that the researchers who make use of NodeMCU often do not refer to it as an open IoT platform; however, this is the case as soon as they are providing a description of it. We note that on Wikipedia, NodeMCU is referred to as an *open-source IoT platform*; however, its official homepage refers to it as *an open-source firmware and development kit*, which we think is an interesting observation and we agree with the latter. This also outlines that researchers tend to get more easy information from the web.

Furthermore, OpenIoT is mainly used by partners and researchers that were part of the project ICT OpenIoT Project FP7-ICT-2011-7-287305 and that its GitHub repository has received no updates since November 2015, which by coincidence correlates well with the end date of project (28 February 2015) as stated by the grant agreement. The requirement of the IoT platform being ready to use and having an active community has gained momentum and become a key criterion in order to be identified as an IoT platform. By coincidence, platforms that either have not had their code updated since December 2015, or with no activity on their website during the same period of time, are considered no longer under active development and therefore do not satisfy the requirement to be identified as *available* IoT platform [32].

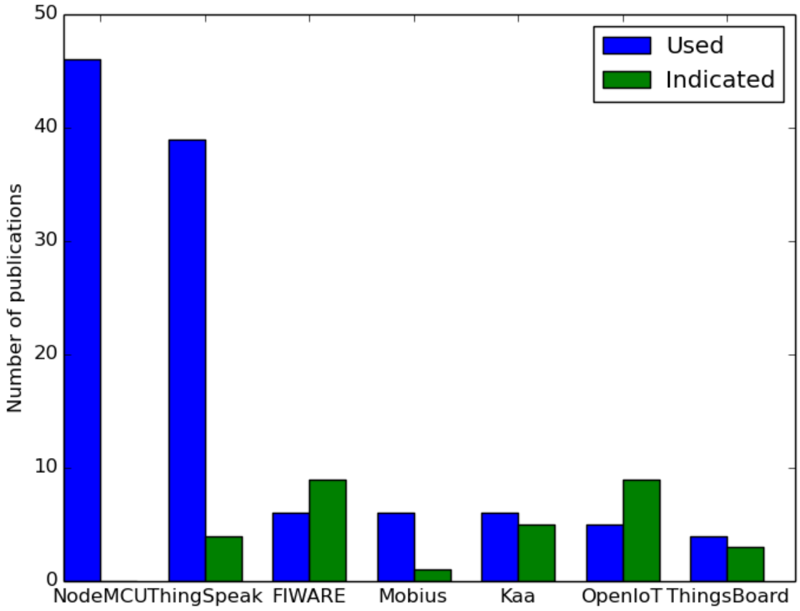

Figure 4. Seven most cited open IoT platforms.

3.3. Q2: Which Are the Openness Types of IoT Platforms?

To answer this question, we used fields F7–F11 from Table 1. From the classified data we were interested to find out what makes the open IoT platform. However, from the F9 field, only three studies provided some directions of openness definitions related to IoT platforms [33–35]. The first study proposes an open IoT service framework [33]. Within this proposal, the authors define their open IoT platform by the following categorization: *Device Platform:* for connecting and cooperating things with open IoT platforms; *Planet Platform:* for server related aspects; *Mashup Platform:* for new integrated services and devices to be available over the Internet; and *Store Platform:* an online store including applications or links for user services.

Observation: Even if the authors claim that they define an open IoT platform [33], there is no clear definition of openness as such.

A very close study related to openness dimensions of platforms, specifically addressing industrial Internet platforms, was analyzed by Menon et al., 2019 [34]. This study provides insights regarding the differences in the degree of platform openness, for instance how open the platform is in terms of the involvement of third-party developers. This involvement varies based on several aspects: (1) the access to information; (2) the rules that allow the usage of a platform; and (3) fee (license fee). The openness dimensions are defined in terms of: *Demand-side user (end user), Supply-side user (application developer)* and *Platform-provider-and sponsor-related openness.* The more open the platform is related to these three dimensions, the more easily different parties can use that platform.

Observation: Even if the authors [34] provide different insights related to openness dimensions of platforms, they do not explicitly define what is an "open" IoT platform. However, an interesting insight out of this study [34] is that stakeholders can play an important role for this matter, thus we bring the stakeholders view later in discussion part of our paper.

The third study by Asemani et al. [35] presents some directions towards understanding IoT platform definitions in general by discussing the main characteristics. In this study, [35], specifically they present high-level features of the open-source projects, such as connectivity/device management, data storage and management, data analysis, data visualization, development tools and platforms, edge/fog computing, integration and interoperation as main characteristics for open-source projects related to IoT platforms.

Observation: Even if the authors [35] provide and place several open-source projects into different characteristics, they do not provide the openness definition and neither the openness types of IoT platforms.

Further on, we analyzed extracted data from F7, F8 (134 used and 56 respectively indicated) and F11. Table 2 shows 25 open IoT platforms that are mapped with the identified openness types. Among them the most common denominator is open-source. For example, 45 studies mark NodeMCU as open-source, and respectively 29 for ThingSpeak. We can consider each openness expression of the different open IoT platforms as a vote for what makes them open, because the specific IoT platform is referred to with different openness types based on author opinions. With Figure 5 we observe that most of researchers consider open IoT platforms from an open-source perspective. Interestingly, for ThingSpeak there are 12 papers in which the authors do not specify the openness type, but just mentioning ThingSpeak as an open IoT platform. Other identified openness types based on "used and indicated" categories of papers are open standards, open APIs, and open data, and some of the papers analyzed do not even specify the openness type of the platforms they use. It is important to highlight that some papers refer to open data in Table 2 for example as compared to open layer as is presented in Table 3 under proposed platforms. Open data we believe leans more toward open standards and sometimes open APIs for example to access data from ThingSpeak, OpenIoT, or FIWARE platforms.

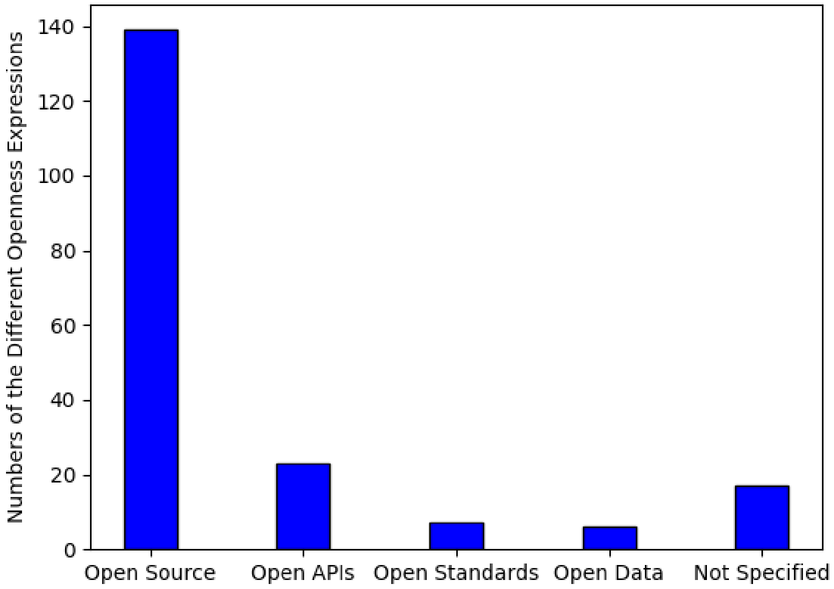

Figure 5. How many times the researchers express a platform as one openness type for the 25 identified IoT platforms in categories "used" and "indicated" among 221 papers.

Table 3. The open IoT platforms identified in "proposed" category and their connection to different openness types.

#	Proposed Platforms	Open-Source	Open Standards	Open APIs	Open Layer	Not Specified
1	ComfortBox	✓				
2	bIoTope		✓	✓		
3	EverySense			✓		
4	HANDYPIA			✓		
5	IoTEP		✓			
6	KIBAN				✓	
7	MONICA		✓	✓		
8	OPEL			✓		
9	OpenIoT			✓		
10	SensorCentral	✓				
11	IoT Manager	✓				
12	Snap4City	✓				
13	SWAMP		✓			
14	viota	✓				
15	Waziup	✓	✓			
16	Liu and Nielsen [36]	✓				
17	Jinbo et al. [37]				✓	
18	Jeon et al. [38]					✓
19	Park et al. [39]					✓
20	Kianoush et al. [40]				✓	
21	Andreev [41]				✓	

Moreover, we analyzed the data extracted from F10—"open IoT platforms proposed" Table 1. Overall, the data from the proposed category of papers shows that their IoT platforms are open. However, we were interested to find out what new open IoT platforms are proposed beside the ones identified under "used and indicated" in Section 3.2 and what is their interpretation related to *openness* types. Thus, overall, the openness types (F11) are derived and categorized from the studies that "used", "indicated" and "proposed" the open IoT platforms, for details see Tables 2 and 3. Among the 28 papers proposing open IoT Platforms, 21 "Proposed Platforms" are offered, and six do not provide a name of the platform (indicated with authorship in Table 3). Based on explicit statement from the papers, interestingly only eight IoT platforms are defined as open IoT platform because of open-source as shown in Table 3, whereas five are because of open standards, another five are related to open APIs, and four are related to open layer. Based on the observation from the analyzed data from the studies, the open layer is intended to integrate different third-party software. However, this kind of functionality could also be provided mostly by open APIs. Compared to open layer, open APIs usually have a more formal format to access and invoke them. Moreover, most of the open APIs can be treated as open layer, but not the opposite. Two studies mention openness in terms of open service and the use of Blockchain as an open database, thus are mapped as *Not Specified* in Table 3. Some platforms have overlapped openness types, like bIoTope, with both open standards and open APIs.

The above openness types are directly extracted from the collected papers in this study. However, to understand the different openness types further, we explain them as follows:

Open-Source has already created a big ecosystem and innovation in the IT industry in general and beyond. The Open-Source Initiative (OSI) provides a clear definition with regards to ten requirements in order to decide what constitutes open-source, for example including free redistribution and accessing source code in terms that anyone can inspect, modify, and enhance it by complying to some basic principles [42]. Moreover, open-source can affect the industry to move faster towards open innovation with the benefit of reducing development costs [12,43].

Open Standards have a wide range of meaning associated with their usage, whereas we refer to a joint definition from the IEEE (Institute for Electrical and Electronics Engineers), ISOC (Internet

Society), W3C (World Wide Web Consortium), IETF (Internet Engineering Task Force) and IAB (Internet Architecture Board). The open standards require five key principles, including cooperation, collective empowerment, availability and voluntary adoption to serve products and services targeted for different market requirements [44]. Open standards are primarily important to provide the support for heterogeneous devices to enable better interoperability [12].

Open APIs are publicly available application programming interfaces that provide developers with programmatic access to a proprietary or open software application or to a web service [45]. Open APIs are usually used by third-party developers.

Open Data should be freely available to everyone to use and republish as they wish, without restrictions from copyright, patents or other mechanisms of control [46].

Open Layer is a technical description rather than a formal term. Based on the context of the related papers, the open layer is considered to be a software layer of the platform that is open for third-party software integration.

Reflecting on our study, we observe that open-source is the most widely accepted openness type as it is more convenient for third-party developers to have a full access to the source code. Open standards, such as that on which FIWARE is based, has some overlap with open APIs; however, they are usually used under different contexts. For example, FIWARE has a FIWARE-NGSI version 2 API in its specification, which is intended to manage the lifecycle of the context information. Moreover, the FIWARE open APIs are slightly different from the ones provided by ThingSpeak; for example, FIWARE APIs are part of the open standards.

Another interesting observation is gleaned by looking at Tables 2 and 3, which reveal that 1 out of 21 proposed open IoT platforms are not widely used ones, besides the OpenIoT platform. This is mainly because the OpenIoT was a funded research project which was mainly used by the involved partners.

4. Discussion

Our results show that there are 25 IoT platforms characterized as open which are categorized under "used" as presented in Table 2. Additionally, 21 IoT platforms categorized under "proposed" as presented in Table 3 are also characterized as "open", summing up to a total of 46 identified open IoT platforms from this study. In general, the type of openness is more evenly distributed. These platforms are used in different domains and implementations, and the most commonly used are NodeMCU and ThingSpeak. Our study also suggests that the most common openness type is open-source, but also open standards, open APIs, and open layers are used in the literature. Furthermore, we take this analysis one step further by investigating the different *openness* types.

4.1. Open-Source vs. Openness of IoT Platforms

As we reflected in Section 3.2, it was interesting to see that the researchers refer to NodeMCU as an open IoT platform. Based on this observation, we decided to study the homepages of the respective IoT platforms in order to compare their self-descriptions (Accessed online 16 April 2020), including the availability requirements, which are provided in Table 4.

Table 4. Comparison of the actual definition of the mostly used open IoT platforms.

Platforms	Original Description	Availability Requirement [32]
NodeMCU	An open-source firmware and development kit that helps you to prototype your IoT product within a few Lua script lines (https://www.nodemcu.com)	Yes
ThingSpeak	Open IoT platform with MATLAB analytics (https://thingspeak.com)	Yes
Mobius	Open-source IoT server platform based on the oneM2M standard. IoT server platform based on Node.js (http://developers.iotocean.org/archives/module/mobius)	Yes
FIWARE	Open-source platform for our smart digital future (https://www.fiware.org)	Yes
KAA	The most flexible IoT platform for your business (https://www.kaaproject.org)	Yes
OpenIoT	Open-source middleware for getting information from sensor clouds, without having to worry about what exact sensors are used (http://www.openiot.eu)	No
ThingsBoard	Open-source IoT platform for data collection, processing, visualization, and device management (https://thingsboard.io)	Yes

First, it is worthwhile to mention that five from the seven most used IoT platforms use the term platform on their homepages. In relation to this, we note that the self-description of NodeMCU states that it is an *open-source firmware and development kit* and not that it is an *open-source IoT platform*. *Second*, we note that the term *open-source* is not used for the ThingSpeak and KAA platforms. In relation to this, it is interesting to note that both started as open-source but then moved to the PaaS model with pricing options. However, it is also important to note that the available community edition from KAA has an active community and does fulfill the *availability requirement* from [32], whereas this does not apply to the open-source version of ThingSpeak, whose codebase has not been updated since November 2015 on GitHub. Even though ThingSpeak is still referred to as an open-source IoT platform, it is mostly used as an open IoT platform from an open APIs perspective. Rather than reusing the source code, most developers use ThingSpeak as a service, e.g., under the paid license options provided by MathWorks. FIWARE is in a similar situation, where even though it is open-source, it is mostly used as an open standard. Reflections such as these have been encouraged in the literature, for example in [47]. *Third*, note that the terms *middleware* and *firmware or development kit* are used to refer to OpenIoT and NodeMCU, respectively. See [48–51] for more information regarding what IoT middleware and IoT platform should accomplish, respectively.

4.2. Defining Openness of IoT Platforms?

Another result of our study is that there are no clear definitions related to the openness of IoT platforms. One of the papers attempts to define the platform aspects only [33], another paper categorizes the openness dimensions of platforms [34], and a final study categorizes some open-source platforms but without providing a definition [35]. Thus, none of them explicitly define what an open IoT platform is. Moreover, in our study we were also interested to identify the openness types of IoT platforms. Our results suggest that the most common openness types of most IoT platforms are related to open-source. Other types identified are open standards, open APIs, open data and open layer-based platforms. However, to further investigate the openness types of IoT platforms we believe it is important to look from a stakeholder view, as identified above [34,52]. Thus, it is essential to further analyze *how important these openness types are from different IoT stakeholder perspectives*.

Some of the most prominent key stakeholders within the IoT ecosystem are categorized as platform providers, application providers, device providers, system integrators and operators [52]. *Platform providers* deliver IoT products and services including IoT enabling capabilities, integration with third-party devices or applications, analytics and so on. *Application providers* usually provide more domain-specific solutions and applications. *System integrators* support end-to-end integration as well as testing. *Device providers* offer embedded devices, sensors, smart devices and appliances and so on [52]. Finally, *operators* provide the network infrastructure and connectivity.

Based on our study results, presented in Tables 2 and 3, several IoT platforms are considered open from different openness types, and this result expresses that the open IoT platform definition indirectly is affected from the different perspectives. We believe that the definition of open IoT platform mainly depends on how the stakeholders use the platform itself with their main concerns. Below we list several insights regarding this issue.

Platform providers often need to develop their own IoT platform based on existing open ones, and open-source is highly beneficial to develop such a platform with full source code-level control, e.g., the famous mobile platform Android [53] is a very good example that is derived from a previous open-source Linux platform and is widely used among different stakeholders and users. Open standards on the other hand do not offer the source code-level implementation. However, platform providers can employ open standards and implement it in their own way, e.g., an agent platform FIPA-OS is implemented based on FIPA (Foundation for Intelligent Physical Agents) agent standards [54]. However, if the openness type of a platform is based on open APIs only, consequently for platform providers that would not be considered open anymore. For example, since ThingSpeak has changed its business model to commercial use, and its source code has not been updated since 2015, the newest edition of it is not considered open for this type of stakeholders anymore. While we believe that application providers can still benefit using it, specifically due the open APIs. Moreover, for platform providers openness can adopt several models that can define the openness in different ways [34]. Thus, *we observe that open-source and open standards are important openness types for platform providers*.

Application providers play an essential role in the IoT ecosystem by providing applications based on open IoT platforms. For them, an IoT platform can be considered "open" as long as it provides an open standard or even just an open API. Whether the IoT platform is open-source or not, it is not fundamental from an application providers perspective. In a study of Fazio et al., [55] FIWARE is used to provide a remote patient monitoring application, e.g., FIWARE is a widely used IoT platform as open standard from application providers' perspective. In another study [51], 12 IoT platforms are chosen to evaluate from application provider viewpoint and four platforms are described as open. However, they are not restricted to open-source and two of them are referred as open APIs. [51]. Moreover, application providers often focus on core developers, third-party developers and data aggregators [34]. Thus, *we observe that open APIs and open standards are important openness types for application providers*.

System integrators usually deal with complex IoT offerings with many moving parts including sensors, devices, connectivity, platform, business logic, applications and users [52]. Thus, system integrators play a unique role to provide end-to-end IoT solutions by integrating different parts, including the open IoT platform. The openness type of an IoT platform for system integrators could be different depending on how the IoT platform is used to deliver final solutions. The system integrators must consider multiple devices and technologies. If the system integrator concerns compatibility primarily, the open standard will be more critical openness type than others. An open standard can help the system integrators to decrease the switching cost to build a better ecosystem in many fields, i.e., in avionics [56] and in robot controllers [57]. From an implementation perspective, open layer, open APIs and open-source could also be considered for system integrators but always depending on their requirements. For example, if the system integrators provide their own IoT platform as a solution, then open-source is significantly more important openness concern. The availability of the source code control allows a system integrator to extend its offering in the areas of support services and it gives the system integrators more business potentials [58]. Thus, *we observe that open standards and open-source play a significant role for system integrators.*

Device providers Compatibility is an essential concern for device providers to support different IoT platforms, devices and other techniques. Therefore, open standards are critical for device providers to define an IoT platform as open. For example, open standards for medical devices play a significant role for medical platforms in these environments [59]. An open layer could also be important for device providers, while open-source and open APIs are usually not relevant. An open platform provided by Sensoria Corporation for distributed sensor networks exploits an open layer as FUSD (User Space Device Drivers) to enable POSIX-standard device file interfaces [60]. The open layer of FUSD can benefit device providers to support many complex features in the same consistent manner [60]. Thus, *we observe that open standards are the most important openness type for this kind of IoT stakeholders*.

Operators Operators mostly do not have a direct relation with open IoT platforms. Thus, *we observe that openness types of IoT platform are not essential for operators*.

For different stakeholders in the IoT ecosystem, the openness of IoT platform obviously has different meanings. The above insights are based on existing literature and our reflection of how the stakeholders can potentially use the IoT platform for their own benefits. Even though the results show that open-source is the mostly referred openness type among the analyzed papers, in this study we observe that open standards play a more critical role for most of the stakeholders in the IoT ecosystem as seen above. Apart from the platform providers, most of the other stakeholders are concerned with open-source in relation to the openness types of IoT platforms. However, open standards sometimes explicitly or not can be transferred from open-source or open APIs as well. A widely accepted open-source IoT platform can also become the standard in the industry.

From the perspective of defining the open IoT platform in the context of different stakeholders' viewpoints, we can adjust these viewpoints among the different identified expressions for open IoT platforms from the analyzed papers, e.g., the change of ThingSpeak from open-source to more open APIs does not make ThingSpeak less open. It is just less open for platform providers and yet even more open and attractive for application providers. Thus, different openness types depend on the stakeholders' needs.

The definition from the proposed perspective can also help the IoT platforms owners to make strategical decisions on their designs based on their relevant stakeholders' demands. For example, if an IoT platform plans to attract more application developers to build more IoT applications on its platform, the open APIs may be already enough. However, if the IoT platform plans to provide wider influence across different domains, open-source and open standard may be a better choice. Based on our results, it is also worth noting that there is an increasing interest of research surrounding the use of the term openness in the IoT domain in recent years.

In summary, the main findings of our study show that open IoT platforms are characterized by different openness types, while the most dominant type is open-source. The most used platforms among the IoT community are NodeMCU and ThingSpeak. Openness types in general are directly influenced from the interpretation of different stakeholder viewpoints. Below we highlight several open issues:

- Since none of the analyzed papers define openness, identifying openness dimensions of IoT platforms remains a challenge to be addressed.
- It is of utmost importance to find a consensus regarding openness among the different stakeholders to avoid confusion, and preferably agree on a formal definition.
- Investigating openness not only from IoT platform perspective, but also considering IoT middleware and frameworks.
- To understand how much openness of IoT platforms has penetrated the field and in which domains, a mapping study of the application domains of the identified open IoT platforms would be useful.

5. Limitations and Threats to Validity

One of the main limitations related to openness is our search string that was focused on open IoT platforms as such, whereas we did not investigate middleware or framework in the context of our study, from which we might miss other relevant data. Other limitations for example can be related to carrying a deeper investigation on how the identified open IoT platforms were used by studying their implementation and additional characteristics as well.

Misunderstandings among the researchers involved in the review process related to search and methods could cause some biased results. For this, the five involved researchers discussed the reliability of this study in its very early stage, at design phase, with the aim to mitigate the bias. In particular, the threat was mitigated through the discussion and refinement of our review protocol before the start of the review process to ensure unbiased results.

Additionally, during the review process we identified several papers that did not provide enough information for us to suitably record the data. Therefore, the researchers met several times and discussed to disambiguate case by case and recorded the data.

Finally, for our study, we limited our search scope to well-known publishers, and that consequently may have led to miss some studies published in other venues. Therefore, to sum up, we do not claim that we collected all existing studies in the literature, but tried to include as many of them as possible according to a systematic method rigorously designed and executed.

6. Conclusions

In this paper, we report the results from our systematic mapping study with the aim to shed some light on what makes an open IoT platform. Overall, we observe the rapid growth of the interest in openness in IoT area.

The goal of our study was to characterize and understand the concept of openness with respect to IoT platforms. In this paper, we provide insights related to this goal. One of the main outcomes shows that in total 46 IoT platforms are often characterized as open. NodeMCU and ThingSpeak are widely adopted platforms among the IoT community. The most common denominator of openness type identified in our study is open-source, followed by open APIs, open standards, open data and open layer. Open-source is the most widely accepted openness type with most of researchers referring the open IoT platform as open-source, as it is more convenient for third-party developers to have a full access to the source code of the platform. Open standards are crucial in our analysis for device compatibility which is also mostly preferred by various stakeholders as seen above.

To conclude, our study shows that open IoT platforms are characterized by different openness types such as open-source, open APIs, and open standards, whereas these types are directly influenced by the demands of different IoT stakeholders. For example, an open IoT platform for application providers can be considered open if it provides an open standard or open APIs, whereas for system integrators open standards are more relevant. For platform providers open-source is more relevant to have a more control level into the platform itself. Having in mind that the IoT platforms are important, the openness aspects are becoming more important from different stakeholder perspectives in terms of enabling new business opportunities that can boost productivity, convenience and open innovation. The insights of this study point out that the open IoT platform definition is related to different openness types; however it is of utmost importance to highlight that this is primarily dependent on diverse stakeholders view.

As a future work, we plan to provide a more formal definition of the open IoT platform rather than a perspective by consulting different stakeholders in detail. The open IoT platform term is frequently used in public and without clear understanding could cause problems like misunderstanding or even wrong strategic decisions. Our future work intends to provide a clearer and deeper understanding of open IoT platforms for the communities. The open issues listed above are also some possible directions of investigation.

Author Contributions: Conceptualization, B.V., Y.D., B.E., P.D. and R.S.; Data curation, B.V. and Y.D.; Investigation, B.V., Y.D. and B.E.; Methodology, B.V., Y.D., B.E., P.D., R.S; Project administration, B.V.; Validation, P.D. and R.S.; Visualization, Y.D. and B.E.; Writing—original draft, B.V.; Writing—review & editing, B.V., Y.D., B.E., P.D. and R.S. 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 number 20140035.

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

References

1. 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]
2. Borgia, E. The Internet of Things vision: Key features, applications and open issues. *Comput. Commun.* **2014**, *54*, 1–31. [CrossRef]
3. Voulodimos, A.S.; Patrikakis, C.Z.; Sideridis, A.B.; Ntafis, V.A.; Xylouri, E.M. A complete farm management system based on animal identification using RFID technology. *Comput. Electron. Agric.* **2010**, *70*, 380–388. [CrossRef]
4. Ancillotti, E.; Bruno, R.; Conti, M. The role of communication systems in smart grids: Architectures, technical solutions and research challenges. *Comput. Commun.* **2013**, *36*, 1665–1697. [CrossRef]
5. Delmastro, F. Pervasive communications in healthcare. *Comput. Commun.* **2012**, *35*, 1284–1295. [CrossRef]
6. Ericsson. More than 50 Billion Connected Devices. Available online: https://vdna.be/publications/Wp-50-Billions.Pdf (accessed on 16 April 2020).
7. Sundmaeker, H.; Guillemin, P.; Friess, P.; Woelfflé, S. Vision and challenges for realising the Internet of Things. *Clust. Eur. Res. Proj. Internet Thing. Eur. Comm.* **2010**, *3*, 34–36.
8. Middleton, P.; Kjeldsen, P.; Tully, J. Forecast: The Internet of Things, Worldwide, 2013. Available online: https://www.gartner.com/en/documents/2625419/forecast-the-internet-of-things-worldwide-2013 (accessed on 16 April 2020).
9. Lin, J.; Yu, W.; Zhang, N.; Yang, X.; Zhang, H.; Zhao, W. A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet Things J.* **2017**, *4*, 1125–1142. [CrossRef]
10. Thomas, I.; Kikuchi, S.; Baccelli, E.; Schleiser, K.; Doerr, J.; Morgenstern, A. Design and implementation of a platform for hyperconnected cyber physical systems. *Internet Thing.* **2018**, *3*, 69–81. doi:10.1016/j.iot.2018.08.012. [CrossRef]
11. 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]
12. Mineraud, J.; Mazhelis, O.; Su, X.; Tarkoma, S. A gap analysis of Internet-of-Things platforms. *Comput. Commun.* **2016**, *89*, 5–16. [CrossRef]
13. Derhamy, H.; Eliasson, J.; Delsing, J.; Priller, P. A survey of commercial frameworks for the internet of things. In Proceedings of the 2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA), Luxembourg, Luxembourg, 8–11 September 2015; pp. 1–8.
14. Hammi, B.; Khatoun, R.; Zeadally, S.; Fayad, A.; Khoukhi, L. IoT technologies for smart cities. *IET Netw.* **2017**, *7*, 1–13. [CrossRef]
15. Kuila, S.; Dhanda, N.; Joardar, S.; Neogy, S. Analytical Survey on Standards of Internet of Things Framework and Platforms. In *Emerging Technologies in Data Mining and Information Security*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 33–44.
16. 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.
17. Weinberg, B. The internet of things and open source. In *Interoperability and Open-Source Solutions for the Internet of Things*; Springer: Berlin/Heidelberg, Germany, 2015; pp. 1–5.
18. 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; p. 36.

19. Petersen, H.; Baccelli, E.; Wählisch, M. Interoperable services on constrained devices in the internet of things. In Proceedings of the W3C Workshop on the Web of Things, Berlin, Germany, 25–26 June 2014.
20. Box, S.; West, J.K. Economic and Social Benefits of Internet Openness. Available online: https://ssrn.com/abstract=2800227 (accessed on 16 April 2020).
21. Ray, P.P. A survey of IoT cloud platforms. *Future Comput. Inform. J.* **2016**, *1*, 35–46. [CrossRef]
22. Farahzadi, A.; Shams, P.; Rezazadeh, J.; Farahbakhsh, R. Middleware technologies for cloud of things: A survey. *Digit. Commun. Netw.* **2018**, *4*, 176–188. [CrossRef]
23. Guth, J.; Breitenbücher, U.; Falkenthal, M.; Leymann, F.; Reinfurt, L. Comparison of IoT platform architectures: A field study based on a reference architecture. In Proceedings of the 2016 Cloudification of the Internet of Things (CIoT), Paris, France, 23–25 November 2016; pp. 1–6.
24. Guth, J.; Breitenbücher, U.; Falkenthal, M.; Fremantle, P.; Kopp, O.; Leymann, F.; Reinfurt, L. A detailed analysis of IoT platform architectures: Concepts, similarities, and differences. In *Internet of Everything*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 81–101.
25. Hejazi, H.; Rajab, H.; Cinkler, T.; Lengyel, L. Survey of platforms for massive IoT. In Proceedings of the 2018 IEEE International Conference on Future IoT Technologies (Future IoT), Eger, Hungary, 18–19 January 2018; pp. 1–8.
26. Petersen, K.; Vakkalanka, S.; Kuzniarz, L. Guidelines for conducting systematic mapping studies in software engineering: An update. *Inf. Softw. Technol.* **2015**, *64*, 1–18. doi:10.1016/j.infsof.2015.03.007. [CrossRef]
27. Kitchenham, B. Procedures for performing systematic reviews. *Keele UK Keele Univ.* **2004**, *33*, 1–26.
28. Basili, V.R.; Caldiera, V.; Rombach, H. The goal question metric approach. *Encycl. Softw. Eng.* **1994**, *2*, 1–10.
29. Harzing, A.W. Publish or Perish. 2007. Available online: https://harzing.com/resources/publish-or-perish (accessed on 7 June 2019).
30. Brereton, P.; Kitchenham, B.A.; Budgen, D.; Turner, M.; Khalil, M. Lessons from applying the systematic literature review process within the software engineering domain. *J. Syst. Softw.* **2007**, *80*, 571–583. doi:10.1016/j.jss.2006.07.009. [CrossRef]
31. Dyba, T.; Dingsoyr, T.; Hanssen, G.K. Applying Systematic Reviews to Diverse Study Types: An Experience Report. In Proceedings of the First International Symposium on Empirical Software Engineering and Measurement (ESEM 2007), Madrid, Spain, 20–21 September 2007; pp. 225–234. doi:10.1109/ESEM.2007.21. [CrossRef]
32. Forsstrom, S.; Jennehag, U.; Österberg, P.; Kardeby, V.; Lindqvist, J. Surveying and Identifying the Communication Platforms of the Internet of Things. In Proceedings of the 2018 Global Internet of Things Summit (GIoTS), Bilbao, Spain, 4–7 June 2018; pp.1–6.
33. Kim, J.; Lee, J.W. OpenIoT: An open service framework for the Internet of Things. In Proceedings of the 2014 IEEE World Forum on Internet of Things (WF-IoT), Seoul, Korea, 6–8 March 2014; pp. 89–93.
34. Menon, K.; Kärkkäinen, H.; Wuest, T.; Gupta, J.P. Industrial internet platforms: A conceptual evaluation from a product lifecycle management perspective. *Proc. Inst. Mech. Eng. Part B: J. Eng. Manuf.* **2019**, *233*, 1390–1401. [CrossRef]
35. Asemani, M.; Abdollahei, F.; Jabbari, F. Understanding IoT platforms: Towards a comprehensive definition and main characteristic description. In Proceedings of the 2019 5th International Conference on Web Research (ICWR), Tehran, Iran, 24–25 April 2019; pp. 172–177.
36. Liu, X.; Nielsen, P.S. Air quality monitoring system and benchmarking. In *Big Data Analytics and Knowledge Discovery*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 459–470.
37. Jinbo, C.; Yu, Z.; Lam, A. Research on Monitoring Platform of Agricultural Product Circulation Efficiency Supported by Cloud Computing. *Wirel. Pers. Commun.* **2018**, 1–15. [CrossRef]
38. Jeon, J.H.; Kim, K.H.; Kim, J.H. Block chain based data security enhanced IoT server platform. In Proceedings of the 2018 International Conference on Information Networking (ICOIN), Chiang Mai, Thailand, 10–12 January 2018; pp. 941–944.
39. Park, D.H.; Bang, H.C.; Pyo, C.S.; Kang, S.J. Semantic open IoT service platform technology. In Proceedings of the 2014 IEEE World Forum on Internet of Things (WF-IoT), Seoul, Korea, 6–8 March 2014; pp. 85–88.
40. Kianoush, S.; Raja, M.; Savazzi, S.; Sigg, S. A cloud-IoT platform for passive radio sensing: Challenges and application case studies. *IEEE Internet Things J.* **2018**, *5*, 3624–3636. [CrossRef]
41. Andreev, I. Advanced open IoT platform for prevention and early detection of forest fires. In *World Conference on Information Systems and Technologies*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 319–329.

42. Initiative, O.S. The Open Source Definition (Annotated), 2007. Available online: https://opensource.org/osd-annotated (accessed on 27 November 2019).
43. Munir, H.; Runeson, P.; Wnuk, K. A theory of openness for software engineering tools in software organizations. *Inf. Softw. Technol.* **2018**, *97*, 26–45. doi:10.1016/j.infsof.2017.12.008. [CrossRef]
44. OpenStand. The Modern Standards Paradigm-Five Key Principles, 2012. Available online: https://open-stand.org/about-us/principles/ (accessed on 27 November 2019).
45. SearchAppArchitecture. What Is an Open API (Public API) and How Does It Work, 2019. Available online: https://searchapparchitecture.techtarget.com/definition/open-API-public-API (accessed on 27 November 2019).
46. Gurstein, M.B. Open data: Empowering the empowered or effective data use for everyone? *First Monday* **2011**, *16*. [CrossRef]
47. da Cruz, M.A.; Rodrigues, J.J.; Sangaiah, A.K.; Al-Muhtadi, J.; Korotaev, V. Performance evaluation of IoT middleware. *J. Netw. Comput. Appl.* **2018**, *109*, 53–65. [CrossRef]
48. Razzaque, M.A.; Milojevic-Jevric, M.; Palade, A.; Clarke, S. Middleware for internet of things: A survey. *IEEE Internet Things J.* **2015**, *3*, 70–95. [CrossRef]
49. Ngu, A.H.; Gutierrez, M.; Metsis, V.; Nepal, S.; Sheng, Q.Z. IoT middleware: A survey on issues and enabling technologies. *IEEE Internet Things J.* **2016**, *4*, 1–20. [CrossRef]
50. Tiwana, A. *Platform Ecosystems: Aligning Architecture, Governance, and Strategy*; Elsevier: Amsterdam, The Netherlands, 2013.
51. Mazhelis, O.; Tyrväinen, P. A framework for evaluating Internet-of-Things platforms: Application provider viewpoint. In Proceedings of the 2014 IEEE World Forum on Internet of Things (WF-IoT), Seoul, Korea, 6–8 March 2014; pp. 147–152.
52. Kar, S.; Chakravorty, B.; Sinha, S.; Gupta, M. Analysis of Stakeholders Within IoT Ecosystem. In *Digital India*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 251–276.
53. Gandhewar, N.; Sheikh, R. Google Android: An emerging software platform for mobile devices. *Int. J. Comput. Sci. Eng.* **2010**, *1*, 12–17.
54. Poslad, S.; Buckle, P.; Hadingham, R. The FIPA-OS Agent Platform: Open Source for Open Standards. Available online: https://www.researchgate.net/profile/Stefan_Poslad/publication/228517710_The_FIPA-OS_agent_platform_Open_source_for_open_standards/links/0deec51b80dcbada60000000.pdf (accessed on 14 April 2020).
55. Fazio, M.; Celesti, A.; Marquez, F.G.; Glikson, A.; Villari, M. Exploiting the FIWARE cloud platform to develop a remote patient monitoring system. In Proceedings of the 2015 IEEE Symposium on Computers and Communication (ISCC), Larnaca, Cyprus, 6–9 July 2015; pp. 264–270.
56. Littlefield-Lawwill, J.; Viswanathan, R. Advancing open standards in Integrated Modular Avionics: An industry analysis. In Proceedings of the 2007 IEEE/AIAA 26th Digital Avionics Systems Conference, Dallas, TX, USA, 21–25 October 2007, p. 2-B.
57. Ferenc, G.; Dimić, Z.; Lutovac, M.; Vidaković, J.; Kvrgić, V. Open architecture platforms for the control of robotic systems and a proposed reference architecture model. *Trans. FAMENA* **2013**, *37*, 89–100.
58. Viljainen, M.; Kauppinen, M. Software ecosystems: A set of management practices for platform integrators in the telecom industry. In *Software Business*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 32–43.
59. Dingler, M.; Dietz, C.; Pfeiffer, J.; Lueddemann, T.; Lüth, T. A framework for automatic testing of medical device compatibility. In Proceedings of the 2015 13th International Conference on Telecommunications (ConTEL), Graz, Austria, 13–15 July 2015; pp. 1–8.
60. Merrill, W.; Sohrabi, K.; Girod, L.; Elson, J.; Newberg, F.; Kaiser, W.J. Open standard development platforms for distributed sensor networks. In Proceedings of the Unattended Ground Sensor Technologies and Applications IV, Orlando, FL, USA, 1–5 April 2002; pp. 327–337.