IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received 10 May 2022, accepted 3 July 2022, date of publication 11 July 2022, date of current version 15 July 2022.
Digital Object Identifier 10.1109/ACCESS.2022.3189660

TOPICAL REVIEW

The Anatomy of IoT Platforms–A Systematic Multivocal Mapping Study

TIAGO G. F. BARROS, (Senior Member, IEEE), ERONIDES F. DA SILVA NETO, (Member, IEEE), JOÃO ALEXANDRE DA SILVA NETO, ANDRÉ G. M. DE SOUZA, VITOR B. AQUINO, AND ERICO S. TEIXEIRA
Cesar School, Recife, Pernambuco 50030390, Brazil
Corresponding author: Tiago G. F. Barros (tgfb@cesar.school)

This work was supported by the Cesar School, Recife, Pernambuco, Brazil.

ABSTRACT Due to the large variety of Internet of Things (IoT) platforms, selecting the right one to implement an IoT solution is a tough task. To mitigate right selection by the developer, this paper presents a Systematic Multivocal Mapping Study on IoT platforms and its main software elements, to define their anatomy considering how they were studied by the market analysts and academia. By using a precise protocol defined on this work, it was possible to select 50 academic articles and industry reports that perform IoT platform descriptions, evaluations and comparisons. As results, this paper identified the most important IoT platforms are AWS IoT, Azure IoT, Watson IoT, PTC ThingWorx and Google IoT. Its main capabilities are Interoperability, Security & Privacy, Developer Support, Data Management, Device Management and Services Management. It was also defined an architectural model with the main platform components highlighted according to their relevance, the main communication models (Publish/Subscribe and REST APIs) and the common API that should be implemented by the IoT platforms.

INDEX TERMS Internet of Things, IoT middleware, IoT platform, multivocal literature review, software architecture, systematic mapping study.

I. INTRODUCTION

The progress of communication technologies and the mass production of cell phones, with their sensors and actuators becoming cheaper, made it possible to embed connectivity, sensors and actuators in everyday things, so that they share data and generate more value for the users [1]. This landscape, called the Internet of Things (IoT), has been extensively studied due to the various challenges it presents. Developing an IoT solution is a complex task because it involves several areas of computer science such as: embedded systems development (hardware and firmware), communication protocols, databases, development of web and mobile applications, data visualization, artificial intelligence and data analytic.

To mitigate this complexity, the research groups in the academy, as well as the ones in the industry, started to build IoT platforms [2]. A recent research listed more than 600 IoT platforms in the market [3], bringing a tough task to developers: *Which platform to choose for developing my IoT solution?*

To answer this question, several aspects of software development must be taken into account. It is a difficult question to answer because it depends not only on the software elements of the various IoT platforms, but also on the functional, non-functional and architectural requirements of the solution to be developed. Considering that the requirements of an IoT solution are specific, this question should be replaced by another, focusing on answer about the IoT platforms themselves.

Therefore, the objective of this work is to identify which are the most relevant IoT platforms nowadays, as well as their main requirements (capabilities), architectural components and operations (APIs - Application Programming Interfaces), the main elements of a software development. Thus, it was defined the main research question:

What is the anatomy of IoT Platforms?

Answering this question will help IoT solution developers as well as IoT platform researchers to understand in depth the

The associate editor coordinating the review of this manuscript and approving it for publication was Rakesh Matam.

main software characteristics of IoT platforms, a high valuable information for their works. This article is not intended to be a comprehensive review of developments in IoT platforms, it follows a precise and well-defined methodology to answer the main research question, bringing in-depth information about the structural organization of IoT platforms.

As result of this work, it was possible to observe that a wide variety of platforms are presented in the literature, with several of them appearing in just one study. However, there is a set of platforms that appears very frequently and that made it possible to define a set of most important IoT platforms, together with their main software elements, both from the perspective of academic researchers and industry analysts.

The reminder of this paper is organized as follows. Section II presents the background concerning IoT and its platforms, as well as the works related to this one. Section III describes the approach for conducting an evidence based research in this study and Section IV describes the protocol for that, and how it was conducted. Section V presents the results and Section VI concludes the paper.

II. BACKGROUND

A. INTERNET OF THINGS

The Internet of Things is a term coined by Kevin Ashton, in 1999, to designate an information network that allows data to be collected automatically from physical objects, through a unique identifier and radio frequency transmission (RFID) [4]. Currently, the term introduces the concept of an environment surrounded by connected things - collecting data through sensors and acting on the environment through actuators - sharing information to improve the way we live and interact with our everyday things [5], [6].

The Internet of Things is a hot research area primarily for two reasons: fist, recent studies [7] points that trillions of dollars will be in the IoT market in the next years; and second because it presents big challenges, such as interoperability, complexity and security [8].

B. IoT PLATFORMS

An IoT platform, in this context, represents a hardware and software infrastructure that implements the generic and common operations of the various IoT solutions [9]. However, unlike the WWW, in which we have a stack of standard protocols and a well-defined client-server architecture, the Internet of Things presents a fragmentation of protocols, motivated by the various connectivity requirements of the things, which are very diverse according to their different use cases. So, this fragmentation of protocols, together with a variety of application areas and software companies that are investing part of their efforts in IoT, also implies in a variety of IoT platforms available on the market [1]. Thus, IoT platforms today are very heterogeneous, with a wide range of functionalities, architectures and integrations with other software components, which makes a deep understanding of this landscape quite difficult.

C. RELATED WORKS

There are already several reviews, evaluations and comparisons for IoT platforms [10]–[14]. The work in [12] compare the most important cloud platforms related to IoT, according to some requirements and performance tests. However, the range of possible platforms is limited to three cloud-based IoT platforms. The study performed in [10] present an overview for architectures, communication technologies, protocols and use cases for IoT. It differs from this work because do not perform a Systematic Literature Review (SLR) for defining these concepts.

The work in [14] combine a set of non-functional and functional requirements together with a set of methods and statistical tests to propose a framework for comparing IoT platforms. Different from this study, the selection process uses K-means to cluster functional requirements and consequently, the platform, but not present the main software elements of the platforms. The paper from [11] presents an overview of worldwide IoT implementation, passing through enabling technologies, protocols, middlewares and use cases. The work also presents a taxonomy for IoT architecture, some simulation tools and the security challenges, however it does not perform an SLR.

The SLR proposed by [13] presents a detailed analysis of 63 different IoT platforms, providing insights of the development process life cycle, the targeted use cases, roles involved in development and modelling activities and modelling languages used. It differs from this study by not presenting the main software elements for IoT platforms. Despite most of the studies in the literature have shown the main features, comparison, and how to choose or develop an IoT platform, there were not found studies that perform a systematic review, taking into account the architectures, communication models and APIs all together.

III. SYSTEMATIC MULTIVOCAL MAPPING STUDY

A Systematic Literature Review aim to investigate the state of the art, presenting an overview of the research area [15]. When the review is presented through classification and counting, it is known as Systematic Mapping Study (SMS) [16]. According to Garousi *et al.* [17], performing an SLR by including the non-peer-reviewed studies (news articles, industry reports and white papers, also called grey literature) is called a Multivocal Literature Review (MLR), to summarize the state-of-the-art and state-of-the-practice in one study.

With these concepts in mind, and considering the nature of this study, it is proposed a Systematic Multivocal Mapping Study (SMMS) to answer all research questions: following instructions from SLR and SMS to investigate the academic literature (peer-reviewed) as well as from MLR to explore industry literature (not peer-reviewed). Thus, this work is based on the SLR, SMS and MLR guidelines [15]–[17], generating the following steps:

- Definition of the protocol for the SMMS
- Perform search and selection

- Perform data modeling and extraction
- Conduct the information synthesis
- Write this report

The first step is the study planning, defined in Section IV. The others are the study execution and were described in Section V.

IV. PROTOCOL DEFINITION

The definition of the protocol for this SMMS was conducted with the definitions of [15]:

- Research questions
- Search strategy
  - Search string
  - Data sources to be used
- Selection criteria
- Data model for extracting information from publications
- Quality assessment checklists
- Synthesis method

A. RESEARCH QUESTIONS

To map the anatomy of IoT platforms, it was decided to conduct this study in two phases:

- ***Phase 1***: to investigate the **literature**, for understanding how the academia and industry studied the IoT platforms, retrieving which platforms and capabilities are most important;
- ***Phase 2***: to investigate the **developer's documentation of most important IoT platforms** from Phase 1, extracting its capabilities, architectures and APIs.

The main objective of this approach was to narrow down the Phase 2 research questions to a small but extremely representative group of IoT platforms.

1) PHASE 1

At the beginning of this research, it was considered that the set of the most relevant IoT platforms, as well as their functionalities, should appear repeatedly in the existing platform studies (e.g. reviews, surveys), and in the works published in the industry literature. That said, to find the most important IoT platforms the following research question was defined:

RQ1: What are the IoT Platforms most studied in the literature?

This research question brings an *objective criterion* for choosing the set of platforms studied in depth at Phase 2: the most studied IoT platforms. The authors also have interest in validate this criterion according to others studies. For doing so, the following research question was defined:

RQ2: What are the criteria for selecting the IoT Platforms in the study?

For selecting the IoT platform that is most adequate to their needs, the developers frequently need to compare or evaluate the existing IoT platforms. For capturing this information, it was defined the following research question:

RQ3: What are the criteria used in the literature to evaluate the IoT Platforms?

Finally, for the IoT platforms requirements, it is necessary to taking into account the requirements from users, represented by capabilities that researchers considered most important while evaluating the platforms; and the requirements from platform developers, represented by the platform capabilities described on its documentation. Then, the requirements research question, RQ4, was split in two: RQ4.1, addressed in Phase 1 (requirements from users) and RQ4.2, addressed in Phase 2 (requirements from developers).

RQ4: What are the most important high level features (Capabilities) for IoT Platforms?

Where the first part of RQ4, was defined as follow:

RQ4.1: What high level features (Capabilities) from IoT Platforms are cited in the literature?

2) PHASE 2

After defined a set of platforms that are the most important (result from RQ1), the Phase 2 will deep dive into their documentation for answering the research questions related to its requirements, architecture and APIs.

For the requirements from platform developers, representing second part of RQ4, the following research question was defined:

RQ4.2: What high level features (Capabilities) the IoT Platforms implement?

For the architecture investigation, the authors are first interested in the communication model that the platform implement. To give this answer, the following research question was defined:

RQ5: What are the communication models that IoT Platforms implement?

Then, the overall architecture for the platform, with its main layers and components also needs to be investigated. To do so, the following research question was defined:

RQ6: What main architectural components the IoT Platforms provide?

Finally, for understanding the most important operations performed by the IoT platforms, it was defined the following research question:

RQ7: What low level features (Operations/APIs) the IoT Platforms implement?

3) FINAL SET OF RESEARCH QUESTIONS

As a summary, Figure 1 presents the final set of research questions, divided into their respective phases and emphasizing the software engineering areas that each research question group belongs to.

Phase	RQ	Question	Category
Phase 1	RQ1	What are the IoT platforms most studied in the literature?	Platforms
Phase 1	RQ2	What are the criteria for selecting the IoT platforms in the study?	Platforms
Phase 1	RQ3	What are the criteria used in the literature to evaluate the IoT Platforms?	Platforms
Phase 1	RQ4*	RQ4.1: What high level features (Capabilities) from IoT Platforms are cited in the literature?	Requirements
Phase 2	RQ4*	RQ4.2: What high level features (Capabilities) the IoT Platforms implement?	Requirements
Phase 2	RQ5	What are the communication models that IoT Platforms implement?	Architecture
Phase 2	RQ6	What main architectural components the IoT Platforms provide?	Architecture
Phase 2	RQ7	What low level features (Operations/APIs) the IoT Platforms implement?	API

*RQ4: What are the most important high level features (Capabilities) for IoT Platforms?

FIGURE 1. Summary of research questions.

TABLE 1. Search string formation.

Internet of Things	*Platforms*	*Literature Reviews*
IoT	Middleware	Comparison
Internet of Things	Platform	Review
Internet of Everything	IoT Cloud	Survey
Web of Things	—	Evaluation

B. SEARCH STRATEGY

It was adopted a different search strategy at each Phase. In the Phase 1, the *literature* is investigated, in peer-reviewed and not-peer-reviewed publications. In Phase 2, the most important platforms' *documentation* is manually investigated.

1) PHASE 1

To answer the research questions from Phase 1, it was defined to perform an *automatic search* on IoT platforms in the academic literature and a *manual search* of the IoT platforms evaluated by the industry, following the guidelines from [15], [16] and [17].

Automatic Search it was decided to search for SLR papers, surveys or reviews that compare, describe or evaluate IoT platforms. After some analysis with a set of keywords being applied to searches on IEEE Xplore, it was defined the following string groups for the search string: Internet of Things, Platforms and Literature Reviews. Thus, it was identified some synonyms for these terms, that are presented in Table 1.

The search string was formed by joining the terms of the same group using an OR operator and by using an AND operator for joining these groups. Then, some searches were performed in IEEE Xplore to validate and it was observed that the terms *Web of Things* and *Evaluation* don't weigh on the results, being removed from the search string. Therefore, the final search string was defined as follows:

("iot" OR "internet of things" OR "Internet of Everything") AND ("platform" OR "middleware" OR "iot cloud") AND ("review" OR "survey" OR "comparison")

Also according to Kitchenham *et al.* [15], it is necessary to define the scope of the literature review. Research questions defined at Phase 1 generally count the number of occurrences of the investigated subject. It was considered that the most important IoT platforms and its requirements appear repeatedly in the studies, and, for this reason, an exhaustive search is not necessary to answer the research questions. Then, it was defined the following data sources for the automatic search:

- IEEE Xplore
- ACM Digital Library
- ScienceDirect
- Springer Link

Manual Search Following guidelines defined in [17], it was decided to use Google search engine for the manual search of comparative studies carried out in the industry. After some evaluations of possible search strings, the following was defined:

"IoT platforms comparison"

Due to Google's algorithm and its indexing capability, a search of such characteristics always returns millions of hits (the search carried out on April 18th, 2022 returned approximately 34,4 million hits). Thus, to limit the evaluation of the hits during the selection phase, it was established the following stopping criterion: go through the result pages

TABLE 2. Selection criteria.

Inclusion Criteria	*Exclusion Criteria*
Journal papers or Conference Papers or industry studies electronically accessible in English or Portuguese	Works not related to IoT software platforms
Published from 2010	Works related to specific IoT platforms (e.g. blockchain platform for IoT)
Present comparisons / surveys of IoT platforms OR	Works focused on specific domain areas (ex: IoT for Industry 4.0, IoT for Health, etc.)
Present IoT platforms functionalities OR	Works focused on the connectivity layer (e.g. network protocol stacks)
Directly answer one of the research questions	Works focusing on specific platform niches (e.g. hardware platforms, open source platforms, etc)
	Publications from sites with low reputation.
	Vendor-dependent publications.

TABLE 3. Extracted information.

Research Question	*Extracted Information*	*Description (search for)*
RQ1	IoT Platform	The name of the platform
RQ2	Selection Criterion	The criterion defined for selecting the platforms in the study
RQ3	Evaluation Criterion	The criterion defined for comparing/evaluating the platforms in the study
RQ4	High Level Feature	High level capability of the platform
RQ5	Communication Model	The communication pattern (e.g. publish/subscribe) and application level protocol (e.g. MQTT) used by the platform
RQ6	Architectural Component	Architecture implemented by the platform, presenting its main components
RQ7	Low Level Feature	Operations (API and SDK functions) performed by the platform
All	Study metadata	Information about the source of information, such as publication year and publication type.

(10 results per page) until reach a page that yields no usable result.

2) PHASE 2

The search in Phase 2 needs to be performed by deep diving in the platforms' documentation. As most of platforms' documentation are web based with a semi-structured content, a manual search is necessary, considering the keywords: *main features, communication models, architectures* and *API*, based on research questions.

The search shall be performed directly in the platform documentation web site, if it allows it (i.e. has a search bar) or by using the Google search engine, associating one of the keywords with the platform name.

C. SELECTION CRITERIA

The selection process described by Kitchenham *et al.* [15] was followed in Phase 1. During the study planning, it was defined that only publications performed after 2010 would be considered for the research. It was also considered that domain specific platforms (e.g. IoT platform for health, IoT platform for home automation) would not be included, because they address specific problems of each of these domains. Works with a focus on the connectivity layer only, or that focused on specific platform niches (e.g. hardware platforms, open source platforms) were also excluded. For the grey literature, it is important to consider the quality of publications. In this way, publications from sources with low reputation or that are vendor-dependant should be excluded. Thus, for the selection of publications, it was defined the selection criteria (inclusion criteria and exclusion criteria) presented in Table 2.

The selection process was conducted according to the following steps:

- Reading the title of the paper and applying the selection criteria;
- If there are doubts about the inclusion or exclusion of the paper, proceed to read the abstract and apply the selection criteria;
- If there are still doubts about the inclusion or exclusion of the paper, it is included and evaluated again in the data extraction phase.

For Phase 2, there is no explicit selection phase for posterior extraction. The documentation returned by the search needs to be read in order to extract the desired information according to the respective research question. If the desired information is not found, the next document returned from the search is examined until the information is found.

D. DATA MODEL

The information extracted from each of the publications and also from platforms' documentation was classified according to the research questions. The extracted information schema and description is shown in Table 3.

E. QUALITY ASSESSMENT

During the selection of publications in Phase 1, it is important to verify that the sources of information are valid and with quality (free of bias, for example). For this, it was applied the guidelines defined on Table 7.3 from [15] for peer-reviewed publications and in Table 7 from [17] for the grey literature in the final selection of publications for Phase 1. It is important to point out that during Phase 2 it does not make sense to perform the quality assessment, since it will be studying the documentation provided by the IoT platforms.

F. DATA SYNTHESIS

Data synthesis was performed using the thematic synthesis method for both Phase 1 and Phase 2 research questions, following the guidelines presented by Cruzes and Dybå [18]. With the thematic synthesis it is possible to group the various

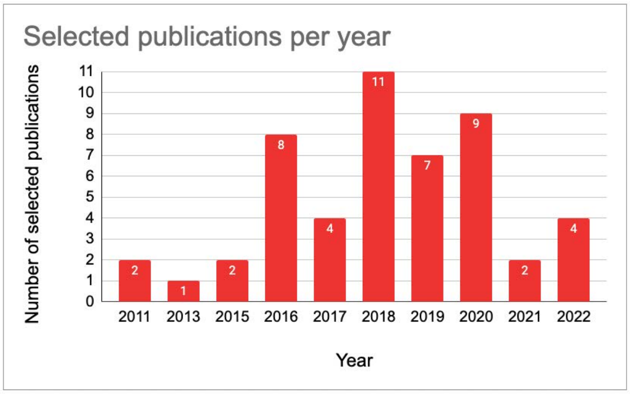


FIGURE 2. Selected publications per year.

TABLE 4. Search and selection results.

Data Source	*Search*	*First Selection*	*Final Selection*
IEEE Xplore	433	22	21
ACM DL	137	2	2
ScienceDirect	169	10	10
Springer Link	317	6	6
Industry Publications	60	13	11
Total	1116	53	50

answers to the research questions into topics of a higher order, identifying patterns (themes) and creating models. This method is the one that best applies to this research due to the descriptive-classificatory nature aof its questions.

V. RESULTS

This section presents the results for the SMMS, based on the analysis of the information extracted from the 50 selected publications [2], [7]–[9], [11]–[14], [19]–[60] and IoT platforms' documentation [61]–[65].

A. SEARCH AND SELECTION RESULTS

For the Phase 1, the automatic search in the IEEE Xplore, ACM Digital Library, ScienceDirect and Springer Link databases returned a total of 1056 papers. The manual search in the grey literature returned a total of 60 publications.

After removing duplicate publications and applying the inclusion and exclusion criteria, it left 40 articles from the peer-reviewed literature and 13 publications from the not-peer-reviewed literature. During the data extraction process, the researchers read the publications and also applied the selection criteria and quality assessment criteria, excluding other set of publications and reaching the final selection numbers presented in the Table 4.

Figure 2 shows the number of selected publications along the years, suggesting that reviews on IoT platforms became a topic of great interest. It is also important to notice how selected publications are distributed by its type, having 20 conference papers, 19 journal papers and 11 industry reports/posts, as depicted in Table 5.

TABLE 5. Publication type.

Publication Type	*Number of Selected Publications*
Conference Papers	20
Journal Papers	19
Industry Reports/Posts	11
Total	50

TABLE 6. Most studied IoT platforms.

Platform	*Number of citations*
Amazon AWS IoT	28
Microsoft Azure IoT	28
PTC ThingWorx	21
IBM Watson IoT	20
Google Cloud IoT	18
Oracle IoT Cloud	14
Xively IoT Platform	14
ThingSpeak IoT Platform	11
OpenIoT	11
SAP IoT Platform	9
LinkSmart	9
FIWARE	9
Cisco IoT Cloud	9
SmartThings	8
GSN	8
Carriots Platform	8
Sensei	7
NimBits	7
Hydra	7
Socrades	6
Particle IoT	6
Kaa IoT Platform	6
GE Predix IoT Platform	6
Bosch IoT Suite	5
OpenRemote	5
NODE-RED	5
GrooveStreams	5
Exosite	5
Ericsson IoT	5
Ayla IoT Platform	5
Number of Platforms cited once	220
Total different Platforms found by this study	325

For the Phase 2, the manual search returned 98 documents mapped, starting from the base documentation page of each studied platform [61]–[65]. Most of them are platform overview documents, developer guides and API reference documents, totalizing thousands of documentation pages analyzed.

B. QUESTION RESULTS

1) PHASE 1

The literature was investigated to answer the research questions from RQ1 to RQ4.1.

RQ1 - What are the IoT platforms most studied in the literature?

The result of this research question presented a list of 325 different IoT platforms found on selected publications. It is important to notice that 220 IoT platforms are cited only once in the studies.

For readability reasons on presenting the list of most studied IoT platforms, this study considered that most important IoT platforms should be cited at least 5 times in the studies. Considering this threshold, the Table 6 lists the most cited IoT

TABLE 7. IoT platforms selection criteria.

Selection Criteria	*Number of citations*	*%*
Non objective criteria	34	68%
Market share	10	20%
Not available	4	8%
SLR	2	4%
Total	50	100 %

platforms in the selected publications (29 IoT platforms), and not the entire list of 325 platforms. A more comprehensive list can be found in Appendix. It is worth noting that the most cited IoT platforms are effectively cloud platform specializations, which demonstrates the importance of cloud support for IoT solutions.

RQ2 - What are the criteria for selecting the IoT platforms in the study?

The results showed that 68% of selected publications does not define any objective criteria for selecting the IoT platforms under study. Some of them use terms like "*selected as an arbitrary way*" [38] or "*we survey available IoT Platforms* [9]" and, either "*a list of (a number) best IoT Platforms*" [53], [59]. Another set of 10 publications, representing approximately 20%, use the *Market Share* criterion to select the IoT platforms for its studies. Some of them use terms like "*we selected according to the reputation of the vendors*" [41] or based on "*IoT Market Analysis*" [56] to define its selection criteria. Only two publications, approximately 4%, define a Systematic Literature Review (SLR) as the selection criteria for the platforms under study. Finally, 4 publications, representing approximately 8%, didn't even mention in the text the criteria used to select the platforms.

Although some of these criteria are acceptable in the contexts of its studies, these results show that a great part of publications may be biased in their evaluations or comparisons, as they do not define an *objective criteria* to select the platforms that will be evaluated or compared. Table 7 summarize the answers for this research question.

RQ3 - What are the criteria used in the literature to evaluate the IoT Platforms?

With this answer, developers can use these criteria to compare the platforms they are evaluating to use. The thematic synthesis for RQ3 extracted text excerpts from selected publications, coded and grouped them in a high order criteria list. A description of the meaning of each evaluation criteria, extracted from the selected publication analysis, in the context of IoT platforms is presented below:

- **Requirements**: in the context of IoT platforms, requirements evaluation criteria means that selected publication performed a comparison between the features or capabilities present on each IoT platform. Either features or capabilities can be abstract characteristics, functional or non-functional requirements, such as: device management, data analytics features or reliability, for example.

TABLE 8. IoT platforms evaluation criteria.

Evaluation Criteria	*Num. of citations*	*%*
Requirements	40	80%
Benchmarks	6	12%
Architecture	6	12%
Security Features	3	6%
User Experience	2	4%
Costs	2	4%
Protocol Availability	1	2%
Application Domains	1	2%
Total	50	100 %

- **Benchmarks**: this evaluation criteria considers that a selected publication perform a performance or metrics comparison between IoT platforms. Performance in this context could be CPU or memory usage, network end-to-end time (the time elapsed between producing and sending a message and receiving that message by the other counterpart) or network message overhead.
- **Architecture**: the architecture evaluation criteria was considered in the studies that performed comparisons on how different IoT architectures have been developed in each IoT platform.
- **Security Features**: some selected publications performed comparisons focusing on security features that each IoT platform implement, such as authentication, authorization, security protocols, encryption algorithms and public-private key infrastructure support.
- **User Experience**: the user experience evaluation criteria, in the context of IoT platforms, takes into account the user opinion regarding the IoT platforms, by performing interviews with IoT platform users, or the features that facilitate the development of IoT solutions, such as over-the-air (OTA) updates, device management or application developer support.
- **Cost**: the selected publications that uses this evaluation criterion compares selected IoT platforms regards its costs for operating IoT solutions, in a model of platform-as-a-service (PaaS).
- **Protocol Availability**: this evaluation criteria takes into account the variety of protocols available in each evaluated platform.
- **Application Domains**: this evaluation criteria compares the selected IoT platforms considering the application domains that each platform support, such as industrial, health, smart cities, etc.

Most publications present more than one evaluation criteria, but Requirements appear in the vast majority (80%) of selected publications as the main evaluation criteria between IoT platforms. In addition to Requirements, other evaluation criteria appeared with the same weight: Benchmarks (12%), and Architecture (12%), showing other concerns of researchers regarding the characteristics of IoT platforms. Finally, mentioned very few times, came Security Features (6%), User Experience (4%), Costs (4%), Protocol Availability (2%) and Application Domains (2%). Table 8 presents the full results for this research question.

TABLE 9. High level features cited.

Capability	*Number of citations*	*%*
Interoperability	37	90.24%
Developer Support	27	65.85%
Security and Privacy	25	60.98%
Data Management	24	58.54%
Device Management	21	51.22%
Event Management	18	43.90%
Services Management	17	41.46%
Performance	15	36.59%
Data Visualization	12	29.27%
Data Analytics	11	26.83%
Costs	9	21.95%
Network Management	9	21.95%
Deployment Management	8	19.51%
Constrained Devices Support	8	19.51%
Reliability	6	14.63%
Cloud Services	6	14.63%
Open Licenses	6	14.63%
Logging/Metrics	5	12.20%
Artificial Intelligence	5	12.20%
Mobile Services Support	2	4.88%
Augmented Reality	1	2.44%
Total	41	100 %

RQ4.1 - What high level features (Capabilities) from IoT Platforms are cited in the literature?

The capabilities extracted from selected publications have great heterogeneity, having been identified 21 different capabilities, between functional, non-functional and architectural requirements. Most publications presented more than ten capabilities, although 9 of the selected publications, about 18%, did not presented any capability at all. It is important to highlight that thematic synthesis method grouped each capability in selected publications into high order capabilities. The same capability synthesis was applied to RQ4.1, RQ4.2 and also RQ4. The description of each capability identified by this study is presented in RQ4 results, because it groups the RQ4.1 and RQ4.2 results.

The most cited capability in RQ4.1 results was *Interoperability*, appearing in more than 90% of selected publications that cite the capabilities. Here, the authors are considering Interoperability in its many levels, as defined by M. Noura *et al.* [66], including network, devices and protocol, semantic, syntactic and platform interoperability. The second most cited capability was *Developer Support*, appearing in more than 65% of selected studies. The third is *Security and Privacy*, appearing in more than 60% of selected publications, showing the relevance of security in IoT platforms.

The next capabilities are related to: *Data* (Data Management, Data Visualization and Data Analytics), *Devices* (Device Management, Event Management) and *Platform Management* in general (Services Management, Network Management and Deployment Management), having also *Costs* and *Performance* appearing in the middle of these groups. Finally, other capabilities such as *Constrained Devices Support*, *Reliability*, support for *Open Licenses*, *Logging and Metrics* among others appeared in the list. Table 9 presents the final results for this research question, with all capabilities cited and its frequency of citation in selected publications.

2) PHASE 2

This phase uses the results from RQ1 to define the most important IoT platforms. Analyzing Table 6, it is possible to observe that the fifth platform (Google Cloud IoT) was cited by 18 publications, which represents 36%, while sixth platform (Oracle IoT Cloud) was cited 14 times, representing 28%. The authors used this distance in number of citations to define the cutoff for the platforms to be studied in Phase 2. Thus, a summary of the 5 most cited IoT platforms is presented below:

Amazon AWS IoT is an IoT cloud platform that provides services to operate IoT devices and create value from the events published by them. It provides a REST API (REpresentational State Transfer API) for provisioning and managing the IoT devices and related capabilities such as metadata, jobs and rules. In addition, the AWS IoT message broker supports the MQTT and LoRaWAN protocols, enabling the interaction between devices and applications through the publish and subscribe of messages. Another aspect of AWS IoT architecture is that it provides end-to-end services, which includes from data analytics to an operating systems for embedded devices. The platform has also a native integration with the AWS cloud services [61].

IBM Watson IoT Platform is a cloud-based set of services that enables gathering data from devices by sending it to the cloud, using MQTT protocol. It has functions for registering and managing the IoT devices, sending data securely and visualizing it in the integrated dashboards. Data is also available in real time and historically through REST APIs so the applications can consume, process and present it according to its needs. The Watson IoT Platform is fully integrated with IBM Cloud, enabling creation of Watson IoT instances directly from Cloud dashboard and integrating it with other IBM Cloud services [62].

Microsoft Azure IoT is a collection of cloud services that connect, monitor, and control IoT assets. The Azure IoT platform provides device SDKs and the IoT Hub, with support for common IoT communication protocols such as HTTP, MQTT, and AMQP; major programming languages (.NET, Node.js, python, C and Java); and multiple software stacks (Azure RTOS, FreeRTOS and BareMetal). The Azure IoT Edge enables moving cloud analytics and custom business logic to devices so that the organization can focus on business insights instead of data management. It is also fully integrated with Azure cloud and all Microsoft services, which ease the deployment of complete IoT solutions. [63].

PTC ThingWorx Industrial Platform is a full device integration cloud platform based on industry-compliant standards. This can be achieved using the ThingWorx connection server based on proprietary websocket protocol (AlwaysOn Protocol) and MQTT. In addition to connect heterogeneous devices, the platform provides visual experiences with data visualization and analysis using descriptive and predictive

TABLE 10. High level features implemented.

Capability	*Number of platforms*	*%*
Security and Privacy	5	100%
Developer Support	5	100%
Data Management	5	100%
Device Management	5	100%
Services Management	5	100%
Data Analytics	5	100%
Interoperability	4	80%
Event Management	4	80%
Cloud Services	4	80%
Logging/Metrics	4	80%
Mobile Services Support	4	80%
Data Visualization	3	60%
Constrained Devices Support	3	60%
Performance	2	40%
Augmented Reality	1	20%
Blockchain Service	1	20%
Total	5	100 %

models. User experience can be enhanced based on augmented reality provided through both web and mobile experiences. Other capability is the expansion of its cloud services by integrating both with Microsoft Azure or Amazon AWS using IoT connectors [64].

Google Cloud IoT Core is an integrated service to manage, connect and store data securely from a few to millions of devices using the structure of Google Cloud. The device connection is established using a bi-directional protocol bridge with MQTT and HTTP endpoints. Its main functions are registration, authentication and authorization, enabling third-party services to any device registered. As a consequence of Google interoperability, implementation of business logic at the edge and data analytic is available. The IoT Core integrates smoothly with all other services present in Google Cloud Platform [65].

RQ4.2 - What high level features (Capabilities) the IoT Platforms implement?

This research question brings the developer point of view to the IoT platform's requirements. The features that are implemented on all studied platforms are: Security and Privacy, Developer Support, Data Management, Device Management, Services Management and Data Analytics. This corroborates with the main features raised by users in RQ4.1, with the exception of Interoperability, which was the most mentioned feature in Phase 1 publications but was not implemented by all platforms studied in Phase 2. Table 10 summarizes all high level features implemented by the studied platforms.

It is noteworthy that the documentation of the platforms studied in Phase 2 presents the high level features in a very summarized way, which caused a certain difficulty to find the information that would answer this research question. This is probably the reason why there are fewer features listed in Table 10 than in Table 9.

RQ4: What are the most important high level features (Capabilities) for IoT Platforms?

This research question synthesize the requirements pointed out by users (RQ4.1) with the requirements cited by platform vendors (RQ4.2). For that, it was considered the percentage that each high level feature achieved in their respective research question and calculated the *relative importance* of each requirement as a simple average of the percentages. As a consequence, due to the smaller amount of elements in the response of RQ4.2, this ended up having a greater weight in this calculation. The results can be seen in Table 11.

TABLE 11. Most important high level features.

Capability	*Relative Importance (%)*
Interoperability	85.12%
Developer Support	82.93%
Security and Privacy	80.49%
Data Management	79.27%
Device Management	75.61%
Services Management	70.73%
Data Analytics	63.41%
Event Management	61.95%
Cloud Services	47.32%
Logging/Metrics	46.10%
Data Visualization	44.63%
Mobile Services Support	42.44%
Constrained Devices Support	39.76%
Performance	38.29%
Costs	21.95%
Network Management	21.95%
Deployment Management	19.51%
Reliability	14.63%
Open Licenses	14.63%
Augmented Reality	11.22%
Blockchain Service	10.00%

In summary, Interoperability, Developer Support and Security & Privacy remain the main features of IoT platforms, to deal with the main challenges from IoT: protocol fragmentation, complexity and security respectively. Considering that the platforms studied in Phase 2 are cloud-based and, in this context, the IoT module of these platforms is a specialization of the cloud platform itself, the other functionalities that appear with greater importance are: Data Management, Device Management and Services Management, precisely the building blocks for implementing an IoT solution (device → data → services).

Then, appear the features that add value to an IoT solution: Data Analytics, Event Management, Cloud Services and Data Visualization. The rest of the features are secondary, but not necessarily negligenced, and serve to contribute to better, more manageable and more robust solutions.

As the thematic synthesis method groups each mentioned capability into high order capabilities (i.e. Data Processing, Data Storage and Data Management itself are grouped under the umbrella of Data Management capability). Below is presented a description of each capability in the context of IoT platforms.

- **Interoperability**: this capability considers all levels of interoperability, from device and protocol interoperability, to cloud and platform interoperability, passing through gateway, data, semantic and syntactic interoperability. It also encompass other terms used in literature as interoperability, such as flexibility, adaptability and heterogeneity.

- **Security and Privacy**: this capability involves the security features, such as identification, authentication, authorization and encryption, and also the privacy related aspects, for example access control, legal and social aspects.
- **Developer Support**: it is a big umbrella that encompass all features that easy the IoT solution development. Examples of such features include: Developer SDK, platform portability, programming languages supported, documentation, number of updates, application marketplace, programming abstractions, modularity and management console.
- **Data Management**: this capability involve the data storage and data processing features, and also the ones related directly to management, such as: data accumulation and cleaning, query processing, data access control and ownership, data sharing and data integration.
- **Device Management**: involves features related to device lifecycle, including device abstractions, virtual or logical devices and digital twin support, asset or fleet management, embedded operating systems, embedded software, sensors and actuators support.
- **Services Management**: this capability considers the features that are related to service handling and control, including service and resource registration and discovery, and also service orchestration.
- **Data Analytics**: besides data management, the data analytics capability handles with support to artificial intelligence engines capable to perform analysis of big amount of data, considering the temporal aspects and relationship between them.
- **Event Management** : this capability encompass event detection and modeling, stream processing and rules engines, the features that brings context awareness to the system.
- **Cloud Services**: it includes the cloud related features, such as cloud hosting, cloud architectures supported and also features such as load balancing and resources provisioning, generally made available in a model of platform-as-a-service.
- **Data Visualization**: this capability involves the features related to graphical user interface of an IoT solution, for example dashboard creation, widget support and report generation.
- **Logging/Metrics**: involves the features related to health monitoring of the system. It includes logging levels, debug support and performance metrics, such as CPU and memory usage, network bandwidth, number of messages sent/received and network delay.
- **Mobile Services Support**: this capability considers the interaction with mobile device applications. So, the features like push notification, Android and iOS SDKs and the use of mobile devices as IoT device abstractions made it to the list.
- **Constrained Devices Support**: it involves the support for devices with limited processing power and communication capabilities. Thus, features like low power small packet protocols, lightweight device SDKs and battery-operated device support are included in this capability.
- **Performance**: the performance aspects of an IoT solution are encompass by this capability. It includes the amount of memory and CPU that are necessary to execute the platform services, the network metrics for packet size, message handling time, response time and message average delay imposed by the protocols. It also includes the cloud performance related aspects, such as scalability, IO metrics, caching and load.
- **Costs**: it involves the pricing and billing model for the IoT platform, generally when it is made available in the platform-as-a-service model. Some selected publications also compare free and paid IoT platforms and the capabilities available in the platform free-tier use.
- **Deployment Management**: this capability deals with the deployment model supported by the platform and includes application provisioning, over-the-air updates, bootstraping and code management.
- **Network Management**: it includes connectivity management features, such as management of all networks supported by the platform (e.g. WiFi management, ZigBee and other IEEE802.15.4 networks management), network credentials provisioning and online/offline detection.
- **Reliability**:this capability involves the capacity of IoT platform to be fault-tolerant, recovering from possible errors of the system, and made it available near to 100% of the time.
- **Open Licenses**: this capability evaluates IoT platform regarding its openness, considering its usage licenses, platform code availability and licensing model that the platform adopts.
- **Augmented Reality**: the capability to integrate with or provide augmented reality functions, applications or tools, presenting architectural components in the platform that are dedicated to it.
- **Blockchain Service**: provides mechanisms for IoT devices to send data and invoke smart contract transactions on blockchain services.

RQ5 - What are the communication models that IoT Platforms implement?

All five platforms implemented the Publish/Subscribe communication model using MQTT as a common protocol, indicating that MQTT is consolidating itself as one of the most supported by IoT platforms. Other common IoT application level protocols, AMQP and CoAP, are supported by just one of the studied platforms. As all IoT platforms studied in this Phase 2 are cloud-based, they also support communication via REST APIs, a standard in the cloud world. In addition to these, some platforms support proprietary full duplex protocols and one also supports the Command and Query Responsibility Segregation (CQRS) [67]

TABLE 12. Communication models.

Platform	*Pub/Sub*	*Req/Rep*	*REST API*	*CQRS*
AWS IoT	X	-	X	-
Azure IoT	X	-	X	-
Watson IoT	X	-	X	X
PTC ThingWorx	X	-	X	-
Google Cloud IoT	X	-	X	-

communication model. Table 12 presents the full list of communication models supported.

It is also important to note that the Request/Reply, another important communication model in IoT world, is not explicitly cited as supported by any of the studied platforms. This is probably because this communication model can be implemented using the Publish/Subscribe, and its implementation is left to solution developers as needed.

RQ6 - What main architectural components the IoT Platforms provide?

A software architecture aims to explain the organization of a software system, presenting its main components, the interaction between them and the interaction between other (external) systems [68]. There are several styles to describe the architecture of an IoT platform. H. Muccini and M. Moghaddam [69] conducted an SMS in IoT architectures, the only one found by the authors, in which they identified that most of IoT architectures were described by the layered style and cloud based style. The layered style defines 3 to 6 layers representing the main component areas for the IoT platform. In the full set of 6 layers, they are: perception, adaptation, network, processing & storage, application and business. The cloud-based style is characterized by a set of services, implemented as components for providing an IoT system.

Based on this, a diagram that mixes the two main styles pointed out (layered and cloud based) was designed by the authors to synthesize the results, considering the architectural components found on each studied IoT platform as well as the result of a brainstorming session performed by the authors to identify the main IoT platform components, based on their experience and knowledge. This diagram is presented in Figure 3 and, as stated in its subtitle, the darker a component is represented, the more platforms have it in their implementation, generating a heatmap of the main architectural components from studied IoT platforms.

It is important to notice that, as the studied platforms are cloud-based, the most common components appear in the upper layers, as the lower layers are most related to hardware. The main components that are present in all studied platforms are the *message broker* (for either the gateway and cloud), *standard IoT protocols, multiple databases support* (relational and NoSQL), *event processing, rules and ML engines, security and identity management, REST APIs, monitoring/logging, data visualization* and, *platform management* in general.

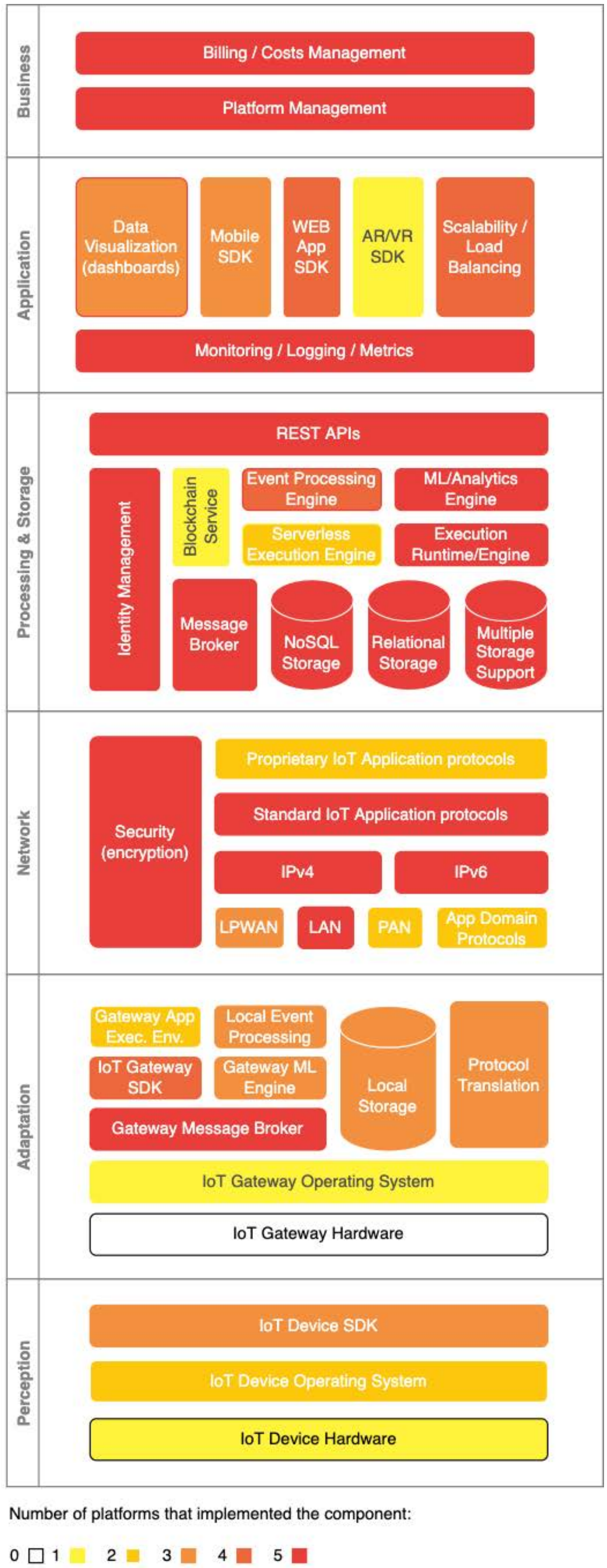


FIGURE 3. Architectural components of IoT platforms.

RQ7 - What low level features (Operations/APIs) the IoT Platforms implement?

Finally this research question brings up a view of the main APIs that the studied IoT platforms implement. The low level

TABLE 13. Low level features implemented.

API	*Number of platforms*	*%*
Authentication API	5	100%
Authorization API	5	100%
Device Management API	5	100%
Device Messaging API	5	100%
Security API	5	100%
Device Schema API	4	80%
Services Management API	4	80%
Data Management API	3	60%
Device Provisioning API	3	60%
Logical Devices API	3	60%
Monitoring/Metrics API	3	60%
Platform Management API	3	60%
Rules Engine API	3	60%
Application Management API	2	40%
Device Monitoring API	2	40%
Event Management API	2	40%
Service Management API	2	40%
Analytics API	1	20%
Augmented Reality API	1	20%
Billing API	1	20%
Connection Management API	1	20%
Device Location API	1	20%
Device Storage API	1	20%
Execution Engine API	1	20%
Gateway Management API	1	20%
Gateway Messaging API	1	20%
Machine Learning API	1	20%
Storage Management API	1	20%
Total	5	100%

features represent the functionalities that the platforms make available to be accessed programmatically through REST endpoints, command-line clients and Software Development Kits (SDKs). Thus, some high level capabilities or some architectural components do not appear in the list of low level features because they are made available through graphical user interfaces (GUI) for platform management or because they are not directly accessible to developers.

Table 13 presents the list of low level features mapped. The APIs that are present in all studied IoT platforms are related to security (authentication and authorization) and devices (device management and device messaging), as they are the core APIs for integrating devices into cloud platforms. Then, other APIs related to advanced device features (such as device schema, provisioning and logical devices); data, services and platform management; monitoring and rules engine appear in the second group. Finally, implemented by only one of the studied IoT platforms, there are APIs for data analytic and machine learning; device location and storage; and billing, among others.

VI. DISCUSSIONS AND CONCLUSION

A. THREATS TO VALIDITY

This study considered that an exhaustive search was not necessary to identify the most important platforms and their requirements. If this statement is not completely true, this work could potentially be affected by publications found in only four data sources. To mitigate this threat, the industry reports were included in this study, bringing another view to the results.

TABLE 14. List of IoT platforms cited at least twice in selected publications.

Platform	*Number of citations*
Amazon AWS IoT	28
Microsoft Azure IoT	28
PTC ThingWorx	21
IBM Watson IoT	20
Google Cloud IoT	18
Oracle IoT Cloud	14
Xively IoT Platform	14
ThingSpeak IoT Platform	11
OpenIoT	11
SAP IoT Platform	9
LinkSmart	9
FIWARE	9
Cisco IoT Cloud	9
SmartThings	8
GSN	8
Carriots Platform	8
Sensei	7
NimBits	7
Hydra	7
Socrades	6
Particle IoT	6
Kaa IoT Platform	6
GE Predix IoT Platform	6
Bosch IoT Suite	5
OpenRemote	5
NODE-RED	5
GrooveStreams	5
Exosite	5
Ericsson IoT	5
Ayla IoT Platform	5
Thinger.IO	4
Temboo Kosmos IoT Platform	4
SiteWhere IoT Platform	4
Paraimpu	4
OpenMTC	4
Mosden	4
EvryTHNG	4
CHOReOS	4
Webinos	3
UBIWARE	3
UBISOAP	3
UbiROAD	3
TheThings.IO	3
Stack4Things	3
SOFIA	3
SensorCloud	3
Salesforce IoT Cloud	3
Open.Sen.Se	3
Mires	3
Jasper Control Centrer	3
IoTivity	3
Hermes	3
Eclipse IoT	3
ClouT	3
CloudPlugs	3
Arrayent Connect Iot Platform	3

TABLE 14. *(Continued.)* **List of IoT platforms cited at least twice in selected publications.**

Platform	*Number of citations*
Arkessa	3
AllJoyn	3
WSO2 IoT	2
WoTKit	2
Ubidots	2
TinyDB	2
ThingsBoard	2
Tago	2
SmartCityWare	2
Smart Santander	2
SiteWhere	2
Sirena	2
Siemens Mindsphere	2
servilla	2
Runes	2
RealTime.IO	2
Ptolemy	2
Prisma	2
Plotly	2
Parse Platform	2
OpenStack	2
MyDevices Cayenne	2
Music	2
M2MLabs Mainspring	2
Losant Platform	2
Lelylan	2
Konker IoT Platform	2
KASOM	2
IRI Voracity	2
Intel IoT Platform	2
In.IoT	2
Impala	2
Huawei OceanConnect	2
Hitachi Lumada	2
Green	2
Eurotech Everyware IoT	2
Echelon	2
DPWS	2
DIAT	2
DeviceHive	2
Cumulocity	2
C3 IoT Platform	2
Axeda	2
Aura	2
AT&T IoT Platform	2
ARM Mbed	2
Altair SmartWorks	2
AirVantage	2
Agilla	2
Number of Platforms cited once	220
Total different Platforms found by this study	325

The Google search engine uses the user's context (browsing and search history, for example) to return more relevant results to this specific user. This causes searches with the same string performed by different people to produce distinct results. This problem was mitigated by performing searches in browsers with anonymous windows (no context information).

B. CONCLUSION AND FUTURE WORKS

This paper presented a Systematic Multivocal Mapping Study to describe the anatomy of IoT platforms. Based on objective selection criteria, were explored 50 publications that evaluate or compare IoT platforms. The information on these publications defined the anatomy of IoT platforms, describing its most relevant requirements, the architecture model highlighting the main components, most common communication protocols, and the main operations that an IoT platform should provide. The results presented allow other studies to apply objective criteria to list IoT platforms, as well as to use the defined protocol to update the most important IoT platforms and their anatomy. In addition, the research questions serve as a basis for comparing them with specific IoT platforms and for developing interoperability models.

APPENDIX
COMPREHENSIVE LIST OF IDENTIFIED IOT PLATFORMS

Table 14 presents a comprehensive list of platforms identified by this study that were cited at least twice in selected publications.

ACKNOWLEDGMENT

The authors would like to thank to Cesar School for supporting this research.

REFERENCES

[1] T. Barros, C. Takahasi, V. Aquino, P. S. Filho, R. Ribeiro, J. A. Neto, C. Batista, P. V. Silva, E. Cavalcante, and T. Batista, "A multi-radio gateway architecture and implementation for consumer electronics," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Las Vegas, NV, USA, Jan. 2019, pp. 1–6.
[2] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, "Middleware for Internet of Things: A survey," *IEEE Internet Things J.*, vol. 3, no. 1, pp. 70–95, Feb. 2016.
[3] *2021 List of IoT Platform Companies*. Accessed: Sep. 14, 2021. [Online]. Available: https://iot-analytics.com/product/list-of-iot-platform-companies/
[4] K. Ashton, "That 'Internet of Things' thing," *RFID J.*, vol. 22, no. 7, pp. 97–114, 2009.
[5] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Jun. 2010.
[6] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, Oct. 2015.
[7] M. A. A. da Cruz, J. J. P. C. Rodrigues, J. Al-Muhtadi, V. V. Korotaev, and V. H. C. de Albuquerque, "A reference model for Internet of Things middleware," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 871–883, Apr. 2018.
[8] D. Rathod and G. Chowdhary, "Survey of middlewares for Internet of Things," in *Proc. Int. Conf. Recent Trends Adv. Comput. (ICRTAC)*, Sep. 2018, pp. 129–135.
[9] J. Mineraud, O. Mazhelisb, X. Suc, and S. Tarkoma, "A gap analysis of Internet-of-Things platforms," *Comput. Commun.*, vols. 89–90, pp. 5–16, Sep. 2016.
[10] D. Kamboj, S. Sharma, and S. Kumar, "A review on IoT: Protocols, architecture, technologies, application and research challenges," in *Proc. 10th Int. Conf. Cloud Comput., Data Sci. Eng. (Confluence)*, Jan. 2020, pp. 559–564.

[11] W. Kassab and K. A. Darabkh, "A–Z survey of Internet of Things: Architectures, protocols, applications, recent advances, future directions and recommendations," *J. Netw. Comput. Appl.*, vol. 163, Aug. 2020, Art. no. 102663.
[12] P. Pierleoni, R. Concetti, A. Belli, and L. Palma, "Amazon, Google and Microsoft solutions for IoT: Architectures and a performance comparison," *IEEE Access*, vol. 8, pp. 5455–5470, 2020.
[13] M. Fahmideh and D. Zowghi, "An exploration of IoT platform development," *Inf. Syst.*, vol. 87, Jan. 2020, Art. no. 101409.
[14] A. Mijuskovic, I. Ullah, R. Bemthuis, N. Meratnia, and P. Havinga, "Comparing apples and oranges in IoT context: A deep dive into methods for comparing IoT platforms," *IEEE Internet Things J.*, vol. 8, no. 3, pp. 1797–1816, Feb. 2021.
[15] B. A. Kitchenham, D. Budgen, and P. Brereton, *Evidence-Based Software Engineering and Systematic Reviews*. Boca Raton, FL, USA: CRC Press, Nov. 2015.
[16] K. Petersen, S. Vakkalanka, and L. Kuzniarz, "Guidelines for conducting systematic mapping studies in software engineering: An update," *Inf. Softw. Technol.*, vol. 64, pp. 1–18, Aug. 2015.
[17] V. Garousi, M. Felderer, and M. V. Mäntylä, "Guidelines for including grey literature and conducting multivocal literature reviews in software engineering," *Inf. Softw. Technol.*, vol. 106, pp. 101–121, Feb. 2019.
[18] D. S. Cruzes and T. Dybå, "Recommended steps for thematic synthesis in software engineering," in *Proc. Int. Symp. Empirical Softw. Eng. Meas.*, Sep. 2011, pp. 275–284.
[19] A. H. Ngu, M. Gutierrez, V. Metsis, S. Nepal, and Q. Z. Sheng, "IoT Middleware: A survey on issues and enabling technologies," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 1–20, Feb. 2017.
[20] Y. J. Dhas and P. Jeyanthi, "A review on Internet of Things protocol and service oriented middleware," in *Proc. Int. Conf. Commun. Signal Process.*, Apr. 2019, pp. 0104–0108.
[21] A. S. Muhammed and D. Ucuz, "Comparison of the IoT platform vendors, Microsoft Azure, Amazon web services, and Google cloud, from users' perspectives," in *Proc. 8th Int. Symp. Digit. Forensics Secur. (ISDFS)*, Jun. 2020, pp. 1–4.
[22] M. A. A. D. Cruz, G. A. B. Marcondes, J. J. P. C. Rodrigues, P. Lorenz, and R. P. Pinheiro, "Performance evaluation of IoT middleware through multicriteria decision-making," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2018, pp. 1–5.
[23] T. Pflanzner and A. Kertesz, "A survey of IoT cloud providers," in *Proc. Int. Conf. Inf. Commun. Technol., Electron. Microelectronics (MIPRO)*, May 2016, pp. 730–735.
[24] J. B. Hoffmann, P. Heimes, and S. Senel, "IoT platforms for the Internet of production," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4098–4105, Jun. 2019.
[25] M. A. A. D. Cruz, J. J. P. C. Rodrigues, K. Saleem, and A. L. L. Aquino, "Towards ranking IoT middleware platforms based on quantitative and qualitative metrics," in *Proc. IEEE First Summer School Smart Cities (SC)*, Aug. 2017, pp. 67–72.
[26] G. Fersi, "Middleware for Internet of Things: A study," in *Proc. Int. Conf. Distrib. Comput. Sensor Syst.*, Jun. 2015, pp. 230–235.
[27] Y. Y. F. Panduman, S. Sukaridhoto, and A. Tjahjono, "A survey of IoT platform comparison for building cyber-physical system architecture," in *Proc. Int. Seminar Res. Inf. Technol. Intell. Syst. (ISRITI)*, Dec. 2019, pp. 238–243.
[28] H. Hejazi, H. Rajab, T. Cinkler, and L. Lengyel, "Survey of platforms for massive IoT," in *Proc. IEEE Int. Conf. Future IoT Technol. (Future IoT)*, Jan. 2018, pp. 1–8.
[29] A. M. Alberti, M. A. S. Santos, R. Souza, H. D. L. Da Silva, J. R. Carneiro, V. A. C. Figueiredo, and J. J. P. C. Rodrigues, "Platforms for smart environments and future Internet design: A survey," *IEEE Access*, vol. 7, pp. 165748–165778, 2019.
[30] A. Azzara, S. Bocchino, P. Pagano, G. Pellerano, and M. Petracca, "Middleware solutions in WSN: The IoT oriented approach in the ICSI project," in *Proc. 21st Int. Conf. Softw., Telecommun. Comput. Netw. (SoftCOM)*, Sep. 2013, pp. 1–6.
[31] J. Guth, U. Breitenbücher, M. Falkenthal, F. Leymann, and L. Reinfurt, "Comparison of IoT platform architectures: A field study based on a reference architecture," in *Proc. Cloudification Internet Things, (CIoT)*, Nov. 2016, pp. 1–6.
[32] R. Sikarwar, P. Yadav, and A. Dubey, "A survey on IoT enabled cloud platforms," in *Proc. IEEE 9th Int. Conf. Commun. Syst. Netw. Technol. (CSNT)*, Apr. 2020, pp. 120–124.
[33] J. Cardoso, C. Pereira, A. Aguiar, and R. Morla, "Benchmarking IoT middleware platforms," in *Proc. IEEE 18th Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, Jun. 2017, pp. 1–7.
[34] S. A. Al-Qaseemi, H. A. Almulhim, M. F. Almulhim, and S. R. Chaudhry, "IoT architecture challenges and issues: Lack of standardization," in *Proc. Future Technol. Conf. (FTC)*, Dec. 2016, pp. 731–738.
[35] A. Farahzadi, P. Shams, J. Rezazadeh, and R. Farahbakhsh, "Middleware technologies for cloud of things: A survey," *Digit. Commun. Netw.*, vol. 4, no. 3, pp. 176–188, Aug. 2018.
[36] A. Botta, W. Donato, V. Persico, and A. Pescapé, "Integration of cloud computing and Internet of Things: A survey," *Future Generat. Comput. Syst.*, vol. 56, pp. 684–700, Mar. 2016.
[37] A. Benayache, A. Bilami, S. Barkat, P. Lorenz, and H. Taleb, "MsM: A microservice middleware for smart WSN-based IoT application," *J. Netw. Comput. Appl.*, vol. 144, pp. 138–154, Oct. 2019.
[38] P. P. Ray, "A survey of IoT cloud platforms," *Future Comput. Inform. J.*, vol. 1, nos. 1–2, pp. 35–46, 2016.
[39] M. Díaz, C. Martín, and B. Rubio, "State-of-the-art, challenges, and open issues in the integration of Internet of Things and cloud computing," *J. Netw. Comput. Appl.*, vol. 67, pp. 99–117, May 2016.
[40] P. P. Ray, "A survey on Internet of Things architectures," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 30, no. 3, pp. 291–319, Jul. 2018.
[41] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," *J. Inf. Secur. Appl.*, vol. 38, pp. 8–27, Feb. 2018.
[42] E. E. Kalmar and A. Kertesz, "What does I(o)T cost?" in *Proc. 8th ACM/SPEC Int. Conf. Perform. Eng. Companion*, 2017, pp. 19–24.
[43] C. Puliafito, E. Mingozzi, F. Longo, A. Puliafito, and O. Rana, "Fog computing for the Internet of Things: A survey," *ACM Trans. Internet Technol.*, vol. 19, no. 2, pp. 1–41, 2019.
[44] S. Bandyopadhyay, M. Sengupta, S. Maiti, S. Dutta, A. Özcan, J. Zizka, and D. Nagamalai, "A survey of middleware for Internet of Things," in *Recent Trends in Wireless and Mobile Networks*. Berlin, Germany: Springer, 2011, pp. 288–296.
[45] S. Banik, I. S. Cardenas, J.-H. Kim, O. Habachi, V. Meghdadi, E. Sabir, and J.-P. Cances, "IoT Platforms for 5G network and practical considerations: A survey," in *Ubiquitous Networking*. Cham, Switzerland: Springer, 2020, pp. 205–225.
[46] T. Teixeira, S. Hachem, V. Issarny, N. Georgantas, W. Abramowicz, I. M. Llorente, M. Surridge, A. Zisman, and J. Vayssière, "Service oriented middleware for the Internet of Things: A perspective," in *Towards a Service-Based Internet*. Berlin, Germany: Springer, 2011, pp. 220–229.
[47] S. Efremov, N. Pilipenko, L. Voskov, and M. Komarov, "Cloud IoT platforms: A solid foundation for the future web or a temporary workaround?" in *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*, S. Balandin, S. Andreev, and Y. Koucheryavy, Eds. Cham, Switzerland: Springer, 2015, pp. 47–55.
[48] R. Sharma, A. Sharma, P. K. Singh, S. Sood, Y. Kumar, M. Paprzycki, A. Pljonkin, and W.-C. Hong, "A review on interoperability and integration in smart Homes," in *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*. Singapore: Springer, 2020, pp. 116–128.
[49] S. Stanovnik, M. Cankar, U. Schwardmann, C. Boehme, D. B. Heras, V. Cardellini, E. Jeannot, A. Salis, C. Schifanella, R. R. Manumachu, D. Schwamborn, L. Ricci, O. Sangyoon, T. Gruber, L. Antonelli, and S. L. Scott, "On the similarities and differences between the cloud, fog and the edge," in *Parallel Processing Workshops*. Cham, Switzerland: Springer, 2020, pp. 112–123.
[50] I. Analytics. *The 25 Best IoT Platforms 2019—Based on Customer Reviews*. Accessed: Sep. 14, 2021. [Online]. Available: https://iot-analytics.com/the-25-best-iot-platforms-2019/
[51] *Comparison of Different Internet of Things Platforms*. Accessed: Sep. 23, 2021. [Online]. Available: https://core.ac.uk/download/pdf/157809905.pdf
[52] *G2. Best IoT Platforms*. Accessed: Sep. 14, 2021. [Online]. Available: https://www.g2.com/categories/iot-platforms
[53] S. T. Help. *10 Best IoT Platforms to Watch Out in 2022*. Accessed: Apr. 18, 2022. [Online]. Available: https://www.softwaretestinghelp.com/best-iot-platforms/
[54] K. Tech. *IoT Platform Evaluation*. Accessed: Apr. 18, 2022. [Online]. Available: https://www.kelltontech.com/file-download/download/public/1114
[55] C. Research. *Counterpoint Research Framework Evaluating the Leading 20 IoT Platforms*. Accessed: Apr. 18, 2022. [Online]. Available: https://www.counterpointresearch.com/microsoft-amazon-clearblade-foghorn-emerge-leading-edge-focused-iot-platforms/

[56] M. Intelligence. *INTERNET OF THINGS (IoT) PLATFORM MARKET—GROWTH, TRENDS, COVID-19 IMPACT, AND FORECASTS (2022–2027)*. Accessed: Apr. 18, 2022. [Online]. Available: https://www.mordorintelligence.com/industry-reports/internet-of-things-platform-market
[57] H. Research. *A Reality Check on who is Winning the IoT Platform Battle*. Accessed: Apr. 18, 2022. [Online]. Available: https://www.hfsresearch.com/research/a-reality-check-on-who-is-winning-the-iot-platform-battle/
[58] J. Guth, U. Breitenbücher, M. Falkenthal, P. Fremantle, O. Kopp, F. Leymann, and L. and Reinfurt, "A detailed analysis of IoT platform architectures: Concepts, similarities, and differences," in *Internet Everything*, B. Di Martino, K.-C. Li, L. T. Yang, and A. Esposito, Eds. Singapore: Springer, 2018, pp. 81–101, doi: 10.1007/978-981-10-5861-5_4.
[59] *Datamation. Best IoT Platforms & Software for 2022*. Accessed: Apr. 18, 2022. [Online]. Available: https://www.datamation.com/networks/iot-platforms/
[60] *DA14. 10 BEST IoT PLATFORMS iN 2018*. IOT TECHNOLOGY FORECAST. Accessed: Apr. 18, 2022. [Online]. Available: https://da-14.com/blog/10-best-iot-platforms-iot-technology-forecast
[61] *AWS IoT Core Documentation*. Accessed: Nov. 3, 2021. [Online]. Available: https://docs.aws.amazon.com/iot/index.html
[62] *IBM Watson IoT Platform*. Accessed: Oct. 13, 2021. [Online]. Available: https://www.ibm.com/docs/en/watson-iot-platform?topic=product-overview-features
[63] *Azure IoT Platform*. Accessed: Nov. 4, 2021. [Online]. Available: https://azure.microsoft.com/en-us/overview/iot/
[64] *ThingWorx Industrial IoT Platform*. Accessed: Oct. 28, 2021. [Online]. Available: https://developer.thingworx.com/en/platform
[65] *Google Cloud IoT Core*. Accessed: Nov. 16, 2021. [Online]. Available: https://cloud.go
ogle.com/iot/docs
[66] M. Noura, M. Atiquzzaman, and M. Gaedke, "Interoperability in Internet of Things: Taxonomies and open challenges," *Mobile Netw. Appl.*, vol. 24, no. 3, pp. 796–809, Jun. 2019.
[67] M. Fowler. (2011). *Cqrs*. Martin Fowler's Blog. [Online]. Available: https://Martinfowler.com/bliki/CQRS.html
[68] D. Garlan and D. E. Perry, "Introduction to the special issue on software architecture," *IEEE Trans. Softw. Eng.*, vol. 21, no. 4, pp. 269–274, Apr. 1995.
[69] H. Muccini and M. T. Moghaddam, "IoT architectural styles: A systematic mapping study," in *Software Architecture*, vol. 11048, C. E. Cuesta, D. Garlan, and J. Pérez, Eds. Cham, Switzerland: Springer, 2018, pp. 68–85.

TIAGO G. F. BARROS (Senior Member, IEEE) received the B.Sc. and M.Sc. degrees in computer science from UFPE, in 2003 and 2007, respectively.

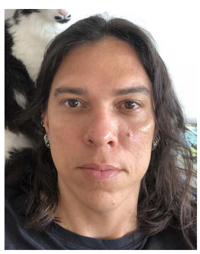
He was a Technician in electronics with ETFPE, in 1998, having issued three patents and leading dozens of software engineering research and development projects. He has been the Chief IoT Engineer at CESAR, responsible for coordinating the CESAR IoT Research Group, since 2014, and design and implement the KNoT network of things meta-platform for the IoT. He is currently the CESAR Representative on ANATEL's Brazilian Commission on Communications (CBC3), that handles the telecommunication standardization in Brazil, being responsible for writing recommendations for ITU-T Study Group 20—the Internet of Things, smart cities, and communities, having published one ITU-T recommendation. He also teaches the IoT, software architecture, and electronic prototyping classes for more than 17 years. He is currently being an Associate Professor with the Cesar School, teaching at master's course in design. He has more than 27 years of experience in software development, with emphasis on the Internet of Things, embedded real-time systems, software and hardware architecture, and communication protocols.

ERONIDES F. DA SILVA NETO (Member, IEEE) received the B.Sc. degree in electronic engineering and the M.Sc. degree in computer science from UFPE, in 2017 and 2019, respectively. He currently works as a Computer Engineer at CESAR, with the development of embedded systems and IoT projects. He has research experience related to the IoT, embedded systems, hardware validation, and anomaly detection in automotive sensors.

JOÃO ALEXANDRE DA SILVA NETO received the B.Sc. degree in information systems from UPE, in 2018. He is currently pursuing the M.Sc. degree in computer science with the Federal University of Pernambuco, Recife, Pernambuco, Brazil. He also works as a Software Engineer at CESAR, playing the role of the Technical Leader of Distributed Systems and DevOps. He has research experience in distributed systems, specially with streaming processing, complex event process (CEP), and computation offloading of CEP in edge computing.

ANDRÉ G. M. DE SOUZA received the B.Sc. degree in electrical engineer from UFCG, in 2017. He currently works as a Software Engineer with focus on PaaS. As a Former Member of the Dedicated Architecture Laboratory (LAD) and (Human–Machine Interface Laboratory (LIHM), he participated in researches related to functional verification for microelectronics devices (LAD) and software development for industry (LIHM). As a Software Engineer, he has relevant work on embedded devices areas such the IoT and digital TV.

VITOR B. AQUINO received the B.Sc. degree in computer engineering from UFPE, in 2018. He currently works as a Software Engineer and the Technical Leader of the Industrial Internet of Things (IIoT) projects at CESAR. He has research experience in the Internet of Things with focus on embedded systems and communication networks.



ERICO S. TEIXEIRA received the B.Sc. and M.Sc. degrees in computer science from UFPE, in 2002 and 2005, respectively, and the dual Ph.D. degree in computational chemistry from UFPE and UF, in 2009. He is currently a Researcher and a Professor with the Cesar School, teaching at bachelor's course in computer science, master's course in design and software engineering, and doctoral course in software engineering. He is also the Coordinator of Natural Computing and Computational Natural Science (C2N2S) and Quantum Application in Technology and Software's (|QATS>) Research Groups.