Internet of Things 7 (2019) 100084

Contents lists available at ScienceDirect

Internet of Things

journal homepage: www.elsevier.com/locate/iot

Review article

Characterizing Internet of Things Systems through Taxonomies: A Systematic Mapping Study

Fahed Alkhabbas[a,b,*], Romina Spalazzese[a,b], Paul Davidsson[a,b]

[a] Department of Computer Science and Media Technology, Malmö University, Malmö 205 06, Sweden
[b] Internet of Things and People Research Center, Malmö University, Malmö 205 06, Sweden

ARTICLE INFO

Article history:
Received 31 January 2019
Revised 1 July 2019
Accepted 3 July 2019
Available online 8 July 2019

Keywords:
Internet of Things (IoT)
Characterization of IoT systems
Systematic Mapping Study (SMS)
Taxonomies

ABSTRACT

During the last decade, a large number of different definitions and taxonomies of Internet of Things (IoT) systems have been proposed. This has resulted in a fragmented picture and a lack of consensus about IoT systems and their constituents. To provide a better understanding of this issue and a way forward, we have conducted a Systematic Mapping Study (SMS) of existing IoT System taxonomies. In addition, we propose a characterization of IoT systems synthesized from the existing taxonomies, which provides a more holistic view of IoT systems than previous taxonomies. It includes seventeen characteristics, divided into two groups: elements and quality aspects. Finally, by analyzing the results of the SMS, we draw future research directions.

1. Introduction

The Internet of Things (IoT) has emerged in our daily life areas like transportation, health-care, surveillance, and smart environments to mention a few [1,2]. New technologies constantly emerge and more and more objects are connected to the Internet every day. Such objects include, for example, sensors, actuators, appliances, and vehicles.

Since Ashton introduced the term “Internet of Things” in 1999 [3], a number of visions have been proposed, including the following ones. Atzori et al. [1] consider the IoT as the outcome of the convergence of three visions, which are thing-oriented, Internet-oriented, and semantic-oriented, respectively. Miorandi et al. [2] presented another vision that builds on the capabilities of IoT things to identify themselves, communicate, and interact. The International Telecommunication Union illustrated the IoT as enabling the “connectivity for anything, from anytime and at anyplace” [4]. Bassi et al. [5] defined the IoT as “things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts”. The following are among the characteristics identified in the final definitions provided by the IEEE Internet Initiative: The IoT “envisions a self-configuring, adaptive, complex network that interconnects ‘things’ to the Internet through the use of standard communication protocols”. In addition, “things have physical or virtual representation in the digital world” where “the representation contains information including the thing’s identity, status, location or any other business, social or privately relevant information” [6].

The existing visions provide a fragmented picture, leading to a lack of common understanding about IoT systems and their constituents. In other words, there is no agreement about the answers to the following questions: What characterizes IoT systems? What are their constituents?

[*] Corresponding author.
E-mail addresses: fahed.alkhabbas@mau.se (F. Alkhabbas), romina.spalazzese@mau.se (R. Spalazzese), paul.davidsson@mau.se (P. Davidsson).

https://doi.org/10.1016/j.iot.2019.100084
2542-6605/© 2019 Elsevier B.V. All rights reserved.

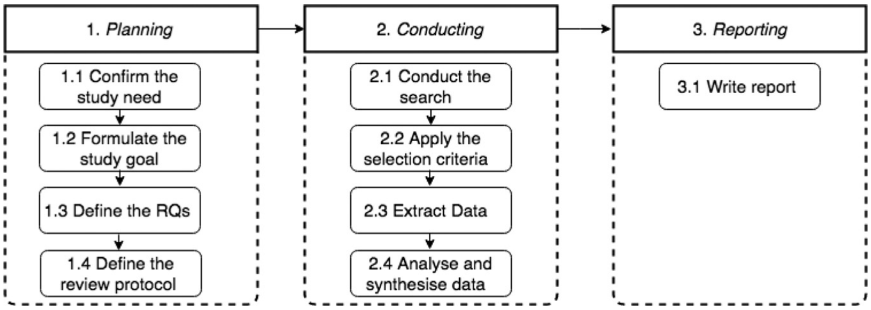
1. Planning
1.1 Confirm the study need
1.2 Formulate the study goal
1.3 Define the RQs
1.4 Define the review protocol
2. Conducting
2.1 Conduct the search
2.2 Apply the selection criteria
2.3 Extract Data
2.4 Analyse and synthesise data
3. Reporting
3.1 Write report

Fig. 1. The applied research methodology.

Table 1
Goal of this study.

Purpose	Identify and synthesize
Issue	Characteristics of
Object	IoT systems
Viewpoint	From researchers and practitioners point of view

A way to fill this gap is to *systematically* analyze existing IoT taxonomies— design artifacts that are used to structure knowledge in complex domains such as the IoT. Also, taxonomies can be considered as reference models that facilitate the engineering and development of different aspects related to IoT systems [7]. In the literature, there are several taxonomies of IoT systems, each of which describes some perspective only. However, to the best of our knowledge, *there is no effort that systematically identifies and analyzes those taxonomies to holistically characterize IoT systems*. This is the goal of our paper.

To this end, the contributions of our paper are summarized as follows:

1. We identify and synthesize characteristics of IoT systems through a *Systematic Mapping Study* (SMS) [8] about existing taxonomies.
2. We organize the characteristics of IoT systems into two categories and formalize their description.
3. We draw future research directions about IoT systems by analyzing the results of the SMS.

The remainder of this paper is organized as follows. Section 2 describes our research method. Section 3 reports the findings of the study. Section 4 discusses the results. Section 5 presents related works. Finally, Section 6 concludes the study and provides future work directions.

2. Research method

We used the well-known guidelines for conducting systematic mapping studies involving three stages [8,9]: *planning, conducting*, and *reporting*. Fig. 1 illustrates the activities carried out at each stage that, excluding Stage 3 (which is self-explanatory), we detail in Sections 2.1 and 2.2, respectively.

2.1. Planning stage

In the planning stage, we carried out the following activities to produce a well-defined review protocol.

(1.1) Confirm the study need. We performed a manual search of IoT systems definitions, constituents, and taxonomies. After a coarse-grain analysis of the results, it was evident that, there is a lack of common understanding about what an IoT system actually is and what it includes. Consequently, we planned our work to contribute to clarifying the existing picture about IoT systems.

(1.2) Formulate the study goal. In the literature, there are several taxonomies that characterize IoT systems from several perspectives. However, to the best of our knowledge, no effort has been made to identify and synthesize existing taxonomic dimensions to characterize IoT systems.

In Table 1, we used the Goal-Question-Metric perspectives to precisely formulate the goal of the study [10]. The audience of the study consists of researchers and practitioners who are interested to (i) contribute to the research about IoT systems and (ii) better understand characteristics of IoT systems and take them into consideration when designing and developing IoT systems.

(1.3) Define the Research Questions (RQs). To achieve the goal of the study, we investigated the following RQs.

RQ1. What are the existing taxonomies of IoT systems?

Objective: by answering this question, we aim to identify the existing taxonomies of IoT systems.

Output: a set of taxonomies which characterize IoT systems.

RQ2. What are the main taxonomic dimensions used for characterizing IoT systems?

```
``taxonomy *[1] IoT *[2](system OR systems OR application OR applications)" OR ``taxonomy *[1] Internet * things
*[2] (system OR systems OR application OR applications)"
OR ``IoT *[1] taxonomy" OR ``Internet * Things *[1] taxonomy" OR ``taxonomy *[1] IoT" OR ``taxonomy *[1] Internet *
things" OR ``IoT *[3] (system OR systems OR application OR
applications) *[2] taxonomy" OR ``Internet * things *[3] (system OR systems OR application OR applications) *[2] taxonomy"
```

Listing 1. Final search string.

[1] number of * incremented from 0 to 5 times (i.e., from * to *****).

[2] number of * incremented from 0 to 1 time.

[3] number of * incremented from 0 to 2 times.

Objective: by answering this question, we aim to identify the main taxonomic dimensions that characterize IoT systems. From now on, we refer to the taxonomic dimensions as characteristics of IoT systems.

Output: a set of IoT systems characteristics.

(1.4) Define the review protocol. This activity includes four sub-activities (a—d) described in the following. We initially produced a version of the protocol that was revised by a colleague expert in conducting empirical studies. Based on the provided feedback and a discussion among the authors, the protocol evolved to its current version.

(a) *Define the search strategy*. To ensure that we cover all relevant studies, we composed our search string using an iterative approach. We first searched Google Scholar with the initial string `taxonomy * (``IoT systems'' OR ``Internet of Things systems'' OR IoT OR ``Internet of Things'')`. The first 100 entries were analyzed by the authors to identify relevant search terms. After that, the search string was refined based on the new identified terms, such as “IoT application(s)” as synonym of “IoT system(s)”. We iterated this process several times to produce the final search string. At each iteration, all new studies were analyzed to check if new search terms were introduced. By the end of this phase, we produced the search string presented in Listing 1. Asterisks in Listing 1 are used as placeholders for unknown or wildcard words. For instance, the string *“IoT * systems”* include phrases like IoT-based systems, IoT-enabled systems, IoT software systems, IoT information systems. To make sure all relevant studies were retrieved, the number of asterisks was incremented until no new studies appeared in the search result set.
We chose Google Scholar as the data source of this study because it is easily accessible and provides reproducible search results. Indexes on other libraries keep evolving, which makes it hard to reproduce search results [11]. The studies that resulted from the search were manually collected in a spreadsheet.

(b) *Generate the selection criteria*. The output of this activity is a well-defined set of inclusion and exclusion criteria. To produce them, we scrutinized the same studies used to produce the final search string. We developed the criteria incrementally, in an iterative process. To attain unbiased criteria, we adopted the mindset of a judge and jury rather than a lawyer [12]. The final criteria are presented below.
Inclusion criteria
I1. Studies that present at least a taxonomy of IoT systems or IoT applications or the IoT. For instance, a study that introduces a taxonomy of IoT things or about the structure of the IoT is included.
I2. Peer-reviewed studies. Some of the results which appear in the search are not peer reviewed (e.g., bachelor or master theses, presentations, tutorials). To ensure the quality of the considered literature, only peer-reviewed studies are included.
I3. Studies written in English. Some studies are not written in English but appear in the search results due to titles or abstracts written in English.
Exclusion criteria
E1. Studies where taxonomies of IoT systems or IoT applications are only introduced as examples. studies that use existing taxonomies as examples and do not explore or extend them are excluded.
E2. Studies that, even though present taxonomies in the context of the IoT, do not introduce dimensions that characterize IoT systems or IoT applications, such as, taxonomies of application domains (e.g., smart cities), threats (e.g., network injection), or attacks on IoT systems (e.g., denial of service).
Eligible studies are those that meet all inclusion criteria and do not meet any exclusion criteria. The eligible studies identify existing taxonomies of IoT systems thus answering RQ1.

Table 2
Data collection form.

ID	Data item
F1	*Title*
F2	*Authors*
F3	*Abstract*
F4	*Year*
F5	*Venue*
F6	*Publication type*
F7	*Study link*
F8	*Root dimension*

(c) *Specify data items*. As shown in Table 2, we identified eight data items that we collect from each of the eligible studies. F1—F6 are used to collect general data about the studies. F7 is used to locate the identified taxonomies. Existing taxonomies have different formats and types and are designed to meet various purposes, so it is difficult to collect all needed information using data sheets. Instead, we used F7 to redirect readers to the identified taxonomies. F8 presents the root dimensions of the taxonomies presented in the eligible studies.

d) *Define a mechanism to analyze and synthesize the data*. We synthesized and showed the distribution of eligible studies based on year and publication type (F4 and F6 in Table 2, respectively), and root dimension (F8). Additionally, to answer RQ2, we analyzed and synthesized the taxonomies identified by the eligible studies by following the mechanism described below.
For each taxonomy, we investigated and understood its objective, root dimension, and first- and second-level dimensions. As a starting point, we considered a taxonomy with root dimension "IoT system". When semantically matching dimensions were identified in other taxonomies (e.g., IoT Applications and IoT Systems, or also IoT Things and Connected Objects), they were properly mapped and merged into a single dimension. Dimensions that were not properly described were excluded. To resolve ambiguities and misinterpretations, weekly clarification and alignment meetings were organized among the authors. This mechanism was applied iteratively until all taxonomies had been explored and mapped.
The answer to RQ2 is provided by the root dimension (IoT system) and the resulting first two levels of sub-dimensions since they describe the main characteristics of IoT systems and their constituents.

2.2. Conducting stage

In the *conducting* stage, we put the protocol in practice by carrying out the following activities.

(2.1) Conduct the search. We searched Google Scholar with the search string illustrated in Listing 1. The search was performed between April 1, 2017, and August 5, 2018. Due to the length of the search string and to the use of different combinations of asterisks, the search activity was carried out in iterations. In each iteration, we used parts of the string and collected the unique studies resulting from the search. Duplicates were identified and matched by titles, authors, and venues of publications. To ensure the tractability of the results, papers presenting the same studies (e.g., workshop papers, conference papers or journal articles) are identified, kept, and mapped to the most general study [13]. In total, we collected 571 unique search results. For each of them, we extracted its title, authors, abstract, and the venue where it is published.

(2.2) Apply the selection criteria. Although in systematic mapping studies selection criteria are often applied on titles, abstracts, and introductions, we noted that many dimensions would be missed if we consider these parts only. Therefore, to obtain comprehensive results, we applied the selection criteria on the full text of all identified studies. The first two authors separately applied the selection criteria on a sample of 100 studies and discussed the results with the third author. One of the authors applied the selection criteria on the rest of the studies. Periodic meetings were organized to resolve uncertainties and discuss doubts. The number of studies that meet the selection criteria is 73.

(2.3) & **(2.4) Extract Data** & **Analyze and synthesize data.** We collected the data items presented in Table 2 from the eligible studies. We applied the synthesis mechanism defined in the review protocol and filled the data item F8 accordingly for all eligible studies.

3. Results

In this section we report the findings of the SMS, including a quantitative analysis of the identified IoT systems taxonomies and a description of the seventeen IoT systems characteristics. To answer RQ1, we surveyed the literature to identify existing taxonomies of IoT systems. Then we applied the inclusion and exclusion criteria presented in Section 2.1 to identify the eligible studies that present taxonomies that characterize IoT systems. The identified *73* eligible studies can be found in the replication package.[1] Fig. 2 shows the distribution of the eligible studies with respect to their year of publication. As

[1] Make sure to use the complete link https://docs.google.com/spreadsheets/d/1HnQ7nPIe6ywJZqY-BWolk8UZcJ4nThaNLsFzkssBnsY/edit?usp=sharing.

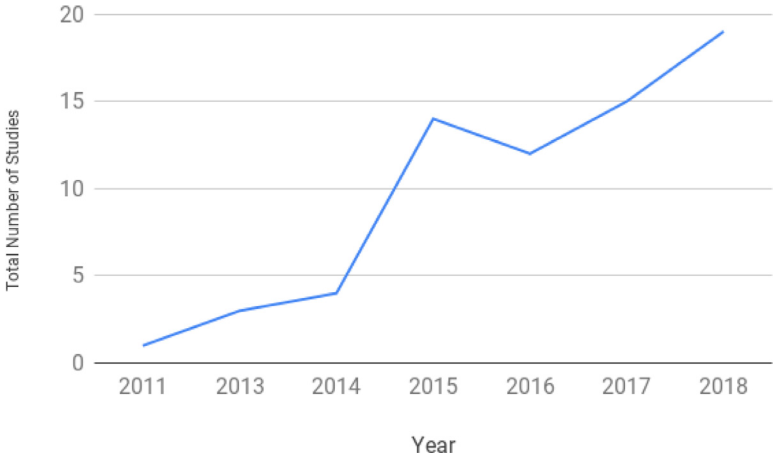

Fig. 2. Distribution of the eligible studies per year.

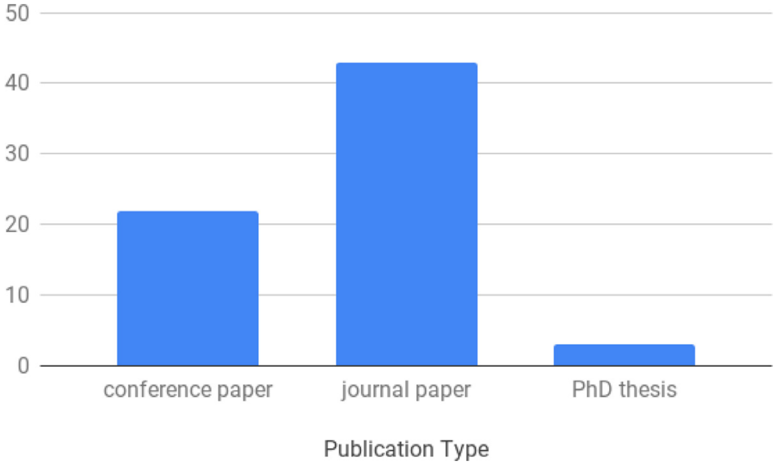

Fig. 3. Distribution of the eligible studies based on publication type.

Table 3
Characteristics of IoT systems.

Quality aspects	Elements
Security	Thing
Privacy	Communication
Trust	Middleware
Interoperability	Data
Scalability	Deployment
Latency	Goal
Reliability	User
	Identifier
	Resource Management
	Collaboration

can be noted, the number of studies presenting taxonomies of IoT systems is increasing rapidly. Most of these studies are published in journals, as shown by Fig. 3.

To answer RQ2, we applied the analysis and synthesis mechanism defined in the review protocol on the set of the eligible studies. As a result, we identified *17 characteristics* of IoT systems and organized them into two categories; they are presented in Table 3 and described in Sections 3.1 and 3.2. We provide a holistic view through a formalization of the IoT systems characteristics in Section 3.3. We grouped the identified characteristics into two categories: (i) *quality aspects* of IoT systems (see Section 3.1) and (ii) *elements* of IoT systems, that is, constituent components (see Section 3.2).

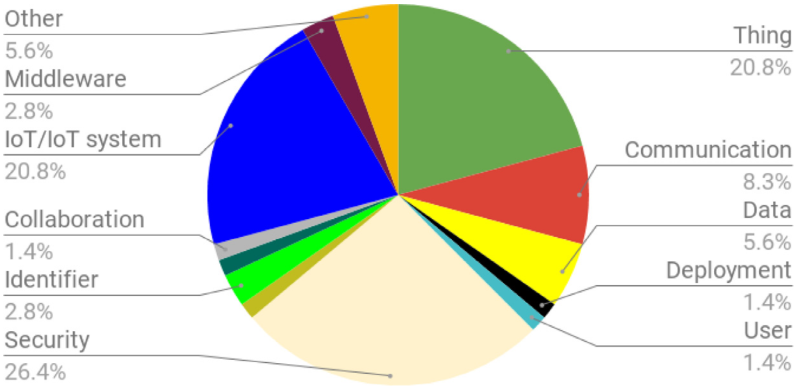

Fig. 4. Distribution of existing taxonomies with respect to their root dimensions.

Fig. 4 illustrates the distribution of the identified taxonomies based on their root dimensions. In the category "other", a root dimension combines security and privacy aspects or characterizes cyber-crimes where the focus is on quality aspects of IoT systems. In this paper, we further analyze the elements of IoT systems, while we plan to analyze the quality aspects and the other characteristics in our future work.

3.1. Quality aspects of IoT systems

Quality aspects are non-functional characteristics of IoT systems. Achieving these qualities depend on different factors related to the elements of IoT systems. For example, the security, privacy, and trust aspects should be guaranteed at different elements including thing, communication, middleware, data, and user. We identified the following quality aspects:

- Security: Characterizes aspects related to an IoT system security—such as confidentiality, integrity, and availability [14].
- Privacy: Characterizes aspects related to the protection of the data of an IoT system [15].
- Trust: Characterizes aspects related to the reliance of users on an IoT system [16].
- Interoperability: Characterizes aspects related to the ability of IoT systems and their constituents to seamlessly communicate and use each other's services [17,18].
- Scalability: Characterizes aspects related to an IoT system's growth, such as the number of participating IoT things and the number of users [19].
- Latency: Characterizes aspects related to the time an IoT system needs to respond to a stimulus (e.g., a user request via an IoT thing) [20,21].
- Reliability: Characterizes aspects related to probability that an IoT system performs failure-free operations (e.g., message delivery) during a specific period of time and in a specific environment [21,22].

As already mentioned, further analysis of these characteristics is planned for future works.

3.2. Elements of IoT systems

Elements represent heterogeneous components of IoT systems. We identified ten elements and their dimensions as described below.

3.2.1. Thing

The IoT extends the concept of the Internet by enabling a wide range of objects (e.g., sensors, actuators, appliances, and vehicles), referred to as "things", to connect to the Internet. Things represent essential building blocks of IoT systems [1,23,24]. In the literature, there is no consensus on what IoT things are. For instance, some studies consider sensors, actuators, tags, smartphones, and everyday objects as IoT things [1,25–27]. In contrast, other studies do not consider tablets, smartphones, and PCs as IoT things [28–31].

There are several taxonomies which characterize IoT things. Barker et al. [32] present a taxonomy of things that constitute IoT ecosystems. Dorsemaine et al. [29] introduce taxonomy of sensors and actuators in the IoT. Trček [26] proposes a two-dimensional taxonomy to characterize IoT things. Muralidharan et al. [33] present another taxonomy of IoT things. Moreover, Ouaddah et al. [34] propose a taxonomy that categorizes IoT things based on their spatial closeness to human. Garcia et al. [27] and Midi [35] classify IoT things based on their processing capabilities (i.e., processing power) and specificity of purpose. Püschel et al. [31] present a multi-layer taxonomy to characterize smart things in the IoT. Yablonsky et al. [36] introduce a taxonomy of innovation of wearable IoT things.

Furthermore, Kale et al. [37] introduce a taxonomy of localization techniques in WSN. Banerjee et al. [38] propose a taxonomy of wearable things in the healthcare domain. Bhatt et al. [39] present a taxonomy of IoT things based on their ability to move. Taivalsaari et al. [40] classify IoT things based on the complexity of their software architectures. Alsamani et al. [41] introduce a set of common characteristics among IoT things. Boyes et al. [42] propose a framework for characterizing IoT things. Mohamed et al. [43] describe a taxonomy which characterizes sensors placement strategies in Wireless Sensor Networks (WSN). Sanchez et al. [25] present a taxonomy of the IoT things supported by the SmartSantander testbed platform.

We analyzed these taxonomies and identified ten dimensions that characterize IoT things as described below.

Type. Things fall under three types:

- Smart things: They are physical objects (e.g., watches, lampposts, and cars) that are turned into smart things by being enriched with communication and processing capabilities that run smart software, they can also be equipped with sensors and/or actuators. Generally, smart things have medium to high processing capabilities [27,32,42].
- Sensors and/or actuators: They perform the sensing and/or actuating functions. They have negligible or lightweight processing capabilities and represent the majority of things in the IoT [27,42].
- Gateways: They are used to support IoT things that posses lightweight processing capabilities and can not process requests individually. They represent the links between various involved things in the system [32]. Such gateways are Raspberry Pi[2] and Arduino[3]. The processing capabilities of gateways range between medium and high.

Function. The functionalities provided by IoT things include sensing, actuating, sensing and actuating, storage, and processing [41,42].

Specificity of goal. The specificity of the goal that IoT things serve ranges between general (e.g., a Raspberry Pi can be used in various types of applications) and specific (e.g., Philips Hue are used for lighting control only) [35].

Level of autonomy. In IoT systems, especially which involve a huge number of IoT things, it is unfeasible to involve human users in every decision. The level of autonomy of an IoT thing is determined by its ability to act independently with(out) human direct intervention to achieve system goals [44]. From this perspective, IoT things can be either non-autonomous, offering no assistance to users; or autonomous, where the level of autonomy ranges between offering a set of suggested actions to users and deciding and acting independently [26,41].

Intelligence. Based on the definitions of intelligence presented in [41,45], the intelligence of a connected thing can be determined by its ability to maximize the probability of satisfying the user goals. The intelligence of connected things ranges from nonexistent to perfectly rational.

Software. The software running on IoT things can be classified based on its type, the possibility of being updated, and the complexity of the Operating System (OS) running it. The identified types of software are proprietary, open source, or hybrid. The software can either be updatable or non-updatable [42]. The complexity of an OS running on a connected thing ranges from simple (e.g., no OS) to complex (e.g., container OS) [40,42].

Relation with user. From a user perspective, IoT things can be classified based on the following [29,34,42,46]:

- User type: Users can be classified into human users and non-human users.
- Spatial closeness to a human user: The identified distance zones between IoT things and humans are intimate (0—0.5 m), personal (0.5—1 m), social (1—4 m), and public (>4 m).
- Interface type: Not all IoT things support interactions with users. Things that interact can have three types of interfaces: active, passive, or active and passive. In active UI, specific parts of a thing are designed to enable interactions with users (e.g., a button). In passive UI, the thing can only communicate with users via its components (e.g., screen, voice, light, etc). In active and passive UI, the thing supports both types of interfaces.
- Usage mechanisms: A user can use a thing directly or via an intermediary (i.e., another thing, e.g., smartphone used to control connected curtains).

Energy. It is one of the critical resources for many IoT things that are mobile and depend on embedded batteries [1,29]. In such cases, the management of energy consumption becomes a major requirement for IoT systems [47]. From this perspective, IoT things can be classified based on the following [29,42,48–50]:

- Power source type: The identified types are harvesting (based on renewable energy such as wind turbines), periodically recharged (e.g., batteries), non-replaceable primary source (i.e., not rechargeable or replaceable), and mains-powered (i.e., unlimited power).
- Operational life time: The identified categories are a few days to weeks (e.g., wearable things such as smart watches), couple of years (e.g., home automation apparatus), exceed several years (e.g., wireless sensors which monitor public infrastructures), or unlimited life span (battery-less devices that depend on ambient power supplies).
- Energy use: The identified categories are normally off, on low power, or always on.

Location. IoT things can be characterized based on their ability to move and on the types of physical locations where they are installed. With respect to the former, IoT things can be static (i.e., stationary) or mobile (i.e., made to move). With respect to the latter, things can be installed in or on different types of physical locations (e.g., buildings, human bodies, and cities) [19,39,42,43].

[2] https://www.raspberrypi.org, accessed on 20/01/2019.

[3] https://www.arduino.cc/, accessed on 20/01/2019

Criticality. IoT things can be classified based on their impact on achieving IoT systems goals and how easy it is to repair or replace them when they are faulty. The former ranges between very low and very high, while the latter can be classified into easy, moderate, and difficult [42].

3.2.2. Communication

Communication, sensing, and actuating technologies represent core aspects in the IoT vision [1,51]. IoT things communicate and collaborate to achieve goals [23,24].

Several taxonomies characterize aspects related to communications in the IoT. Fuqaha et al. [52], Srinidhi et al. [53], and Poluru et al. [54] propose taxonomies of IoT communication protocols. Mashal et al. [55] introduce criteria for comparing communication protocols. Antonić et al. [21] present a taxonomy which characterizes publish-subscribe based middlewares in the context of smart cities.

Moreover, Rahman et al. [56] present a taxonomy of architectural aspects in IoT systems development frameworks. The presented taxonomy characterizes communication protocols in the IoT.

Pozza et al. [57] propose a taxonomy of neighbor discovery approaches for opportunistic networking in the IoT. Pflanzner et al. [19] introduce a taxonomy of network requirements in IoT applications. Barker et al. [58] demonstrate a taxonomy of IoT sensor nodes networks. Mehmood et al. [59] devise a taxonomy of IoT-based smart cities, which characterizes communications in the IoT. Further, Mohamed et al. [43] demonstrate a taxonomy that characterizes data transmission mechanisms in WSN applications.

We analyzed these taxonomies and identified five dimension that characterize communications in the IoT as described below.

Involved parties. Communications can be made between humans and machines (H2M), machines and machines (M2M), machine and servers (M2S), and servers to servers (S2S) [52]. We classify these types into two categories: humans to things and things to things.

Nature. Communications can be made in the real-time or near real-time. Data can also be stored and communicated (a)synchronously [42,43].

Initiation. Communications among IoT things can be initiated by the sending thing, receiving thing or either of them [42].

Protocol. Communication protocols enable IoT things to interconnect and communicate [55]. The IoT involves a large number of heterogeneous things that adapt to various communication protocols [47]. Protocols can be classified into three categories: perception layer protocols (e.g., Bluetooth low energy), network layer protocols (e.g., RPL), and application layer protocols (e.g., MQTT) [53].

Protocols can also be classified from other perspectives, such as standardization, discovery capabilities, architectural styles, constrained environment suitability, and range [19,21,52,55–57]. Communication protocols can be standard (e.g., the Hypertext Transfer Protocol [HTTP]) or non-standard (e.g., HomeKit). Discovery capabilities enable IoT systems to identify available things at a specific point in time in a specific location. Architectural styles specify protocol design patterns (e.g., publish/subscribe). Some protocols can support constrained environments with respect to, for example, energy consumption, processing capabilities, and unreliable networks.

Network. IoT systems constituents are inter-connected by networking and communication technologies [47]. Communication networks can be characterized by, for instance, their speed, frequency, message size, and type. The network speed, can be slow, medium or fast based on messages size and frequency rates. IoT systems can exploit several types of networks such as LAN, WLAN, WAN [19,59].

3.2.3. Middleware

A middleware is a software component that operates between operating systems and applications; it is responsible for providing reusable solutions for common issues including heterogeneity, security, interoperability, et cetera [60].

Mashal et al. [55] discuss an existing taxonomy of IoT middleware. Antonić et al. [21] introduce a taxonomy to compare the CUPUS middleware and Mosquitto broker. Son et al. [61] propose a taxonomy of IoT and Internet of Computing (IoC) technologies and identify two types of IoT middlewares.

We analyzed these taxonomies and identified seven dimensions that characterize an IoT middleware as described below.

Type. An IoT middleware can be service oriented or application oriented [61].

Architecture. An IoT middleware can have a centralized or decentralized architecture [21].

Openness. An IoT middleware can be open or close. An open middleware supports, for example, open software standards, interoperability, and portability [21,55].

Context awareness. An IoT middleware can either support or not support context awareness. If context awareness is supported, an IoT middleware can discover and track IoT things at runtime, for instance. This feature can be exploited to enable IoT systems to cope with the dynamicity of the IoT environment [21,55].

Query language expressiveness. The expressiveness of the queries supported by an IoT middleware can range between limited (e.g., publish/subscribe queries), and expressive (e.g., CUPUS queries) [21].

Things management. An IoT middleware can either support or not support managing IoT things (e.g., turning things on/off) [21].

Data processing support. An IoT middleware can either support or not support processing the data generated by IoT things [21].

3.2.4. Data

Atzori et al. [1] consider the semantic-oriented vision as one of the three visions that converge to represent the IoT paradigm. IoT systems collect data, analyze it, and act accordingly. The number of things connected to the Internet is increasing exponentially[4]. Consequently, the amount of generated and communicated data can be vast. Therefore, mechanisms are needed to support data representation, organization, search, exchange, storage, ownership, visualization, et cetera [1,2,51,62].

Qina et al. [63] and Siow et al. [64] present taxonomies which characterize data in the IoT. Santofimia et al. [65] demonstrate an approach for defining the semantics of IoT data. Verma et al. [66] propose a taxonomy of data analytics. Karim et al. [67] introduce a taxonomy of big data management issues and principles for participatory sensing.

We analyzed these taxonomies and identified six dimensions which characterize data in the IoT as described below.

Type. IoT data types can be textual, time-series, geospatial, numerical, categorical, and multi-modal (i.e., videos, images, and text) [64].

Source. The sources of data in the IoT can be sensors, social media, documents, users/crowd, web, graphs, and knowledge bases to mention a few [64].

Generation. The aspects related to the generation of data in the IoT include volume, velocity, dynamicity, and heterogeneity. Volume is concerned with the size of the data (i.e., small scale, medium scale, or large scale). Velocity is concerned with the data generation rates (i.e., slow, medium, or fast). Dynamicity is concerned with whether the data is generated in dynamic contexts (e.g., where things can join or leave systems suddenly). Heterogeneity is concerned with the diversity of the data (i.e., data could be homogeneous or heterogeneous) [64].

Quality. The aspects related to the quality of data in the IoT include redundancy, uncertainty, and variability. Redundancy is concerned with repetitions in the data. Uncertainty is concerned with the noise, missing readings, precision and accuracy of the data. Variability is concerned with the possibility to interpret the data differently within a specific context. Data quality ranges between low and high based on its redundancy, uncertainty, and variability [63,64].

Processing. Data is automatically processed to deduce knowledge and generate actionable insights [64]. In general, data processing techniques can be classified into historical and proactive. In the former, historical data is processed to obtain insights about IoT systems. In the latter, data is processed to provide predictive and actionable insights about the system [64,66].

Distribution. Data can be stored and processed at IoT things level (i.e., in the Edge), local network level (i.e., in the Fog), or in the Cloud [64].

3.2.5. Deployment

The system deployment process is defined as the sequence of activities for setting up a system into its execution environment and making it available for use [68]. Few studies explore the deployment aspect of IoT systems. Roman et al. [69] introduce a taxonomy of IoT systems architectures based on the distribution of systems processing capabilities and the collaboration schema among systems constituents. Rahman et al. [56] present a similar taxonomy of architectural aspects in IoT programming frameworks focusing on the deployment aspect.

There are three types of computing paradigms where the capabilities of IoT system can reside, namely, Cloud, Fog, and Edge [70]. In the Cloud Computing Paradigm, processing and storage capabilities reside in the cloud. In the Fog Computing Paradigm, processing and storage capabilities reside in more constrained devices that are closer to the edge of the network. In the Edge Computing paradigm, processing capabilities reside in IoT things [56,69].

We analyzed these taxonomies and identified four dimension that characterize IoT systems deployment as described below.

Distribution approach. IoT systems can be deployed in centralized or decentralized approaches. In centralized approaches, data is retrieved and processed, and decisions are made by central entities. In decentralized approaches, different entities can retrieve and process the data and there is no central entity where decisions are made [69].

Control deployment. This dimension characterizes an IoT system based on the paradigm where its control function resides. The control function decides the behaviour of available things and responds to user requests. An IoT system control function can reside in the Cloud, Fog, or Edge [56]. Cloud-based IoT systems can have more powerful processing capabilities but also higher latency rates compared to Fog- or Edge-based systems. Fog-based systems have less processing capabilities than cloud-based systems but have less latency rates. Compared to the others, Edge-based systems have the least latency rates but also have limited processing capabilities [56].

Thing management deployment. This characterizes an IoT system based on the paradigm where its thing management function resides. The things management function is responsible for maintaining IoT things configurations and life cycles. Configurations specify how things are configured to join IoT systems. A management function can reside in the Cloud, Fog, or Edge [56].

Storage deployment. This dimension characterizes an IoT system based on the paradigm where its storage function resides. The storage function is responsible for collecting and storing IoT data. A storage functions can reside in the Cloud, Fog, or Edge [56].

[4] Ericsson Mobility Report, https://www.ericsson.com/assets/local/mobility-report/documents/2017/ericsson-mobility-report-june-2017.pdf, accessed on 20/01/2019.

3.2.6. User

The IoT is expected to emerge in almost every aspect of our daily life. Consequently, it will have a major impact on the community [1]. The IoT will provision new "*always responsive services*" which shall satisfy users' needs [2].

Despite the fact that the user aspect is prominent in the IoT, few taxonomies explore it. Chasaki et al. [71] present a taxonomy of the IoT and identify the user as a key entity. Barker et al. [32] introduce another taxonomy for the IoT and identify two types of IoT systems users. Fritsch et al. [16] propose a taxonomy of interaction scenarios from end users' perspective.

We analyzed these taxonomies and identified the below dimensions that characterize users in the IoT.

Type. IoT systems users can be human or non-human. Human users exhibit free will and have emergent and unpredictable goals, whereas non-human users are (semi) autonomous agents that perform actions based on the permissions granted by human users [32].

Goal. A characterization of user goals is presented in Section 3.2.7.

Perceivable configurations. The perceivable interaction scenarios from end users' perspective are classified based on the identity of the systems with which the users interact. The identified categories are as follows [16]:

- Anonymous systems: For instance, using a smartphone, a user connects to a train station network.
- A system managed by a known party: For instance, using a smartphone, a user connects to her mother's health monitoring system.
- Application specific federation: A federation is a set of IoT things connected to form a trusted group [72]. An example of this category is an engineer who connects to a network of the machines in the manufactory where she works.
- Several federations that might overlap: For instance, using a smartphone, a user browses trains schedules and buys tickets.

User interface type. The different types of interfaces a user can use to interact with IoT things are presented in Section 3.2.1.

3.2.7. Goal

Despite the fact that the goal aspect is prominent for IoT systems, very few taxonomies explore it. Ahmed et al. [73] present a taxonomy which categorizes the various objectives of smart environments. Mohamed et al. [43] propose a taxonomy which characterizes the goals of WSN applications. We analyzed these taxonomies and identified the below dimensions that characterize goals in the IoT.

Type. The types of IoT systems goals include, for instance, monitoring, reducing costs, and improving utilization, etc [43,73]. We categorized different IoT systems goals into two main categories: monitoring and monitoring and control. In the former, IoT systems collect, possibly process, and view data. In the latter, the systems can also change the state of their environments.

User. Like other systems, IoT systems are developed to achieve user goals. A characterization of IoT users is presented in Section 3.2.6.

3.2.8. Identifier

Identification mechanisms are considered among the main enabling technologies of the IoT [1]. To support the dynamic discovery and tracking of IoT things, they should be uniquely identifiable [74]. Challa et al. [74] propose a taxonomy of identifiers in the IoT. Boujezza et al. [75] present a taxonomy of user identification management models in the IoT. We analyzed these taxonomies and identified the below dimension that characterizes identifiers in the IoT.

Type. The identified types of identifiers in the IoT are: things identifiers, communications identifiers, users identifiers, and systems identifiers [74].

3.2.9. Resource management

IoT resources can be classified into things-based resources (e.g., energy levels, storage, and processing capabilities) and network-based resources (e.g., load balancers and traffic analyzers) [76]. Chowdhury et al. [76] proposed a taxonomy of resource management activities in the IoT which comprises the three dimensions described below.

Resource discovery. Discovering available IoT resources in order to consume their services can be achieved by using e.g., resource directories or search engines; both techniques rely on Uniform Resource Identifiers (URI) to uniquely identify resources.

Resource provisioning. Techniques for partitioning available resources efficiently are exploited to ensure a high utilization rate. Such techniques include virtualization and containers.

Resource scheduling. Techniques for dynamically distributing workloads on discovered and provisioned resources include big data-based and little data-based techniques. The former techniques often rely on cloud computing infrastructures, while the latter techniques rely on fog computing infrastructures.

3.2.10. Collaboration

Inspired by the notion of goals and collaboration in socio-technical systems, Eris et al. [77] propose a taxonomy which characterizes the collaboration aspect in IoT systems. The proposed taxonomy comprises the six following dimensions:

Involved parties. The parties that collaborate to achieve IoT systems goals are IoT things or users.

Goal. This refers to the goal of collaboration among things and users; see Section 3.2.7 for more details about IoT systems goals.
Data. This refers to data exchanged among things and users while collaborating to achieve goals; see Section 3.2.4 for more details about data in the IoT.
Complexity. This is the main dimension explored by the taxonomy presented in [77]. It is concerned with the level of autonomy of things, the data aggregation dependency, the number of shared parameter, and the interdependence among involved parties. Details about the level of autonomy of things can be found in Section 3.2.1. The data aggregation rate is the number of IoT things that communicate to realize the collaboration; it ranges between low (less than 5) and high (more than 20). The number of shared parameter equals the count of the distinct data parameters exchanged among the involved parties; it ranges between low (less than 5) and high (more than 20). Further, the interdependence among the involved parties refers to the level of dependencies among their tasks. It can be pooled, where parties do not synchronize their tasks; sequential, where the output of a task becomes the input of another task; and reciprocal, which is similar to the sequential but the parties also have to deal with unexpected situations [78].
Physical properties. They are concerned with the mobility of IoT things and the relation between the things and their users; see Section 3.2.1 for more details about these dimensions.
Network properties. They are concerned with the boundaries of the collaborators private and social networks, the interactions among them, and the level of alignment among their goals.

3.3. A characterization of IoT systems

Leveraging the presented characteristics, an IoT system S is more formally described as $S =< E, Q >$ where E is a tuple describing the *elements* of an IoT system and Q is a tuple describing its *quality aspects*. According to the description in Section 3.2, $E =< T, C, M, D, DP, U, G, I, R, CL >$ where:

- T is a set of *things* t_i, $|T| \geq 2$, and each t_i has as sub-characteristics type t, function f, specificity of goal g, level of autonomy a, intelligence i, software s, relation with users r, energy e, location l, and criticality c.
  More formally, $t_i =< t, f, g, a, i, s, r, e, l, c >$.
- C is a non-empty set of *communication links* c_i and each c_i includes as sub-characteristics involved parties i, nature t, initiation in, protocol p, and network n. More formally, $c_i =< i, t, in, p, n >$.
- M is a set of *middleware* m_i each having as sub-characteristics type t, architecture a, openness o, context awareness c, query language expressiveness q, things management m, and a data processing support d. More formally, $m_i =< t, a, o, c, q, m, d >$.
- D is a set of *data* d_i, and each d_i has as sub-characteristics type t, source s, generation g, quality q, processing p, distribution l. More formally, $d_i =< t, s, g, q, p, l >$.
- DP is a set of *deployment configurations* dp_i where each dp_i has as sub-characteristics distribution approach d, control deployment c, thing management deployment m, and storage deployment s. More formally, $dp_i =< d, c, m, s >$.
- U is a set of *users* u_i and each u_i has as sub-characteristics type t, goal g, perceivable configuration p, and interface type i. More formally, $u_i =< t, g, p, i >$.
- G is a set of *goals* g_i and each g_i is characterized by type t and user u. More formally, $g_i =< t, u >$.
- I is a set of *identifiers* i_i where each i_i is characterized by type t. More formally, $i_i =< t >$.
- R is a set of *resource management mechanisms* r_i and each r_i has as sub-characteristics resource discovery d, resource provisioning p, resource scheduling s. More formally, $r_i =< d, p, s >$.
- CL is a set of *collaboration aspects* c_i where each c_i includes as sub-characteristics involved parties i, goal g, data d, complexity c, physical properties p, and network properties n. More formally, $c_i =< i, g, d, c, p, n >$.

We plan to provide a more formal description of the tuple Q in future work.

4. Discussion

As shown in Fig. 2, the number of the taxonomies proposed to characterize IoT systems and their constituents has been increasing. The majority of these taxonomies are presented in papers that are accepted in journals, as shown in Fig. 3. In addition, as presented in Fig. 4, many focus on security aspects of IoT systems. This might be due to the following reasons. IoT systems are expected to emerge in all aspects of our daily life. Those systems can monitor sensitive data (such as health parameters) and control operations where there is no room for errors (such as in self-driving cars) or operations that can be costly (such as turning on district heating). Therefore, considerable efforts are dedicated to investigate the security of IoT systems since the early stages. A threat to the validity of this observation could be that researchers from the security discipline are more used to propose taxonomies than researchers from other disciplines.

As can be noted in Fig. 4, the most explored elements of IoT systems are IoT thing, communication, and data, respectively. The reason behind focusing on the thing element might be because it adds a physical dimension that makes IoT systems different from software systems. This might also justify the focus on the communication and data elements as enabling a huge number of things that can be mobile and resource constrained to communicate and managing and exploiting the vast data that can be generated represent core aspects in the IoT [1,2,51,62].

Fig. 4 also shows that some elements of IoT systems—such as goal, user, collaboration, and deployment—have not been sufficiently explored yet. Although there are few studies that characterize such elements, based on our expertise and discussions with our industrial partners, such elements represent core characteristics of IoT system and we believe that they deserve much more attention and investigation. Other future research direction concern the quality aspects of IoT systems. Notably, the list of quality aspects identified in this study is not comprehensive as there are several important quality aspects of IoT systems that are not included—such as adaptability, usability, availability, accuracy, and elasticity [20]. As already mentioned, the proposed characterization is based on the existing literature. It could be extended by involving practitioners and investigating realistic case studies.

5. Related work

An initiative to provide a comprehensive definition, which aims at addressing all features, of the IoT is presented in [6]. Atzori et al. [1] presented a paradigm for the IoT based on the convergence of three visions: the thing oriented vision, semantic oriented vision, and Internet-oriented vision.

In the context of taxonomies, several works characterize IoT systems; however, these taxonomies are either defined at an abstract level (e.g., [51,71,79,80]) or take specific perspectives or categories of IoT systems (e.g., [19,42,43,81]). Mountrouidou et al. [82] proposed a taxonomy that aims at facilitating the understanding of IoT ecosystems. The taxonomy classifies IoT devices based on their architectural characteristics and is developed having a security mindset. Moreover, the authors provided an algorithm to validate the completeness, precision, and timelessness of the proposed taxonomy. Whereas they focus on the individual IoT devices, we are taking a system perspective leading to a more holistic view of IoT systems. Moreover, we have made a systematic study analyzing existing taxonomies in the literature.

Conceptual models for IoT systems have been proposed in the literature. Bauer et al. [83] presented a UML model for the IoT domain. Patel et al. [84] introduced a conceptual model for IoT applications. Ciccozzi el al. [85] built on [83,84] to propose a conceptual model for mission-critical IoT systems. These models capture to different extents the dimensions identified in this study; however, none of them captures all the identified (sub)dimensions.

6. Conclusions and future work

Existing characterizations of the IoT lead to a fragmented picture and a lack of common understanding of IoT systems and their constituents. To fill this gap, we identified seventeen characteristics of IoT systems through a Systematic Mapping Study that leverages existing taxonomies. We organized the characteristics into two categories: elements and quality aspects of IoT systems. The proposed characterization represents a step towards the standardization of a universal schema for characterizing IoT systems. Additionally, we provided a formal characterization of IoT systems by exploiting the identified characteristics. We also presented insights about the directions of future research concerning IoT systems.

Among future work, efforts are needed to investigate the elements of IoT systems that seem not to be well-researched such as user, goal, and deployment. Moreover, for some of the presented dimensions, such as the intelligence and the level of autonomy of a thing, further analysis is required to specify clear and objective categories or metrics. Additionally, further studies are underway to analyze the quality aspects of IoT systems.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

The authors would like to thank Dr. Ivano Malavolta for his review and feedback about the protocol. This work is partially financed by the Knowledge Foundation through the Internet of Things and People research profile (Malmö University, Sweden).

References

[1] L. Atzori, A. Iera, G. Morabito, The internet of things: a survey, Comput. Netw. 54 (15) (2010) 2787–2805.
[2] D. Miorandi, S. Sicari, F.D. Pellegrini, I. Chlamtac, Internet of things: vision, applications and research challenges, Ad Hoc Netw. 10 (7) (2012) 1497–1516.
[3] K. Ashton, That 'internet of things' thing. RFID J., 2009.
[4] I. Peña-López, et al., in: ITU internet report 2005: the internet of things, 2005.
[5] A. Bassi, G. Horn, Internet of things in 2020: a Roadmap for the future, Eur. Comm. 22 (2008) 97–114.
[6] R. Minerva, A. Biru, D. Rotondi, Towards a definition of the internet of things (IoT), IEEE Internet Initiat. 1 (2015) 1–86.
[7] R.C. Nickerson, U. Varshney, J. Muntermann, A method for taxonomy development and its application in information systems, Eur. J. Inf. Syst. 22 (3) (2013) 336–359.
[8] K. Petersen, R. Feldt, S. Mujtaba, M. Mattsson, Systematic mapping studies in software engineering, in: EASE, 8, 2008, pp. 68–77.
[9] S. Keele, et al., Guidelines for performing systematic literature reviews in software engineering, in: Technical report, Ver. 2.3 EBSE Technical Report. EBSE, SN, 2007.
[10] V. Caldiera, H.D. Rombach, The goal question metric approach, Encyclop. Softw. Eng. 2 (1994) (1994) 528–532.

[11] M. Kuhrmann, D.M. Fernández, M. Daneva, On the pragmatic design of literature studies in software engineering: an experience-based guideline, Empir. Softw. Eng. (2016) 1–40.
[12] R.F. Baumeister, Writing a literature review, in: The Portable Mentor, Springer, 2013, pp. 119–132.
[13] C. Wohlin, P. Runeson, M. Höst, M.C. Ohlsson, B. Regnell, A. Wesslén, Experimentation in Software Engineering, Springer Science & Business Media, 2012.
[14] A. Mosenia, N.K. Jha, A comprehensive study of security of internet-of-Things, IEEE Trans. Emerg. Topic. Comput. 5 (4) (2017) 586–602.
[15] G. Rosner, Privacy and the Internet of Things, Ph.D. thesis, University of Nottingham, 2016.
[16] L. Fritsch, A.-K. Groven, T. Schulz, On the internet of things, trust is relative, in: AmI Workshops, Springer, 2011, pp. 267–273.
[17] J. Kiljander, A. D'elia, F. Morandi, P. Hyttinen, J. Takalo-Mattila, A. Ylisaukko-Oja, J.-P. Soininen, T.S. Cinotti, Semantic interoperability architecture for pervasive computing and internet of things, IEEE access 2 (2014) 856–873.
[18] M. Noura, M. Atiquzzaman, M. Gaedke, Interoperability in internet of things: taxonomies and open challenges, Mobile Netw. Appl. (2018) 1–14.
[19] T. Pflanzner, A. Kertész, A taxonomy and survey of IoT cloud applications, EAI Endors. Trans. Internet Things 3 (12) (2018) Terjedelem–14.
[20] M. Ashouri, P. Davidsson, R. Spalazzese, Cloud, Edge, or Both? Towards decision support for designing IoT applications, in: The Fifth International Conference on Internet of Things: Systems, Management and Security (IoTSMS 2018), 2018.
[21] A. Antonić, M. Marjanović, P. Skočir, I.P. Žarko, Comparison of the CUPUS Middleware and MQTT protocol for smart city services, in: 2015 13th international conference on Telecommunications (ConTEL), IEEE, 2015, pp. 1–8.
[22] J. Radatz, A. Geraci, F. Katki, IEEE standard glossary of software engineering terminology, IEEE Std. 610121990 (121990) (1990) 3.
[23] E. Borgia, The internet of things vision: key features, applications and open issues, Comput. Commun. 54 (2014) 1–31.
[24] D. Giusto, A. Iera, G. Morabito, L. Atzori, The internet of things: 20th tyrrhenian workshop on digital communications, Springer Science & Business Media, 2010.
[25] L. Sanchez, L. Muñoz, J.A. Galache, P. Sotres, J.R. Santana, V. Gutierrez, R. Ramdhany, A. Gluhak, S. Krco, E. Theodoridis, et al., Smartsantander: IoT experimentation over a smart city testbed, Comput. Netw. 61 (2014) 217–238.
[26] D. Trček, Lightweight protocols and privacy for all-in-silicon objects, Ad Hoc Netw. 11 (5) (2013) 1619–1628.
[27] A. Gonzalez-Garcia, A. Alvarez-Alvarez, J. Pascual-Espada, O. Sanjuan-Martinez, J.M.C. Lovelle, B.C.P. G-Bustelo, Introduction to devices orchestration in internet of things using SBPMN, Int. J. Interact. Multimedia Artif. Intell. 1 (4) (2011).
[28] A. Kees, A.M. Oberländer, M. Röglinger, M. Rosemann, Understanding the Internet of Things: A Conceptualisation of Business-to-Thing (B2T) Interactions, in: ECIS, 2015.
[29] B. Dorsemaine, J.-P. Gaulier, J.-P. Wary, N. Kheir, P. Urien, Internet of things: a definition & taxonomy, in: Next Generation Mobile Applications, Services and Technologies, 2015 9th International Conference on, IEEE, 2015, pp. 72–77.
[30] E. Bucherer, D. Uckelmann, Business models for the internet of things, Architect. Internet Thing. (2011) 253–277.
[31] L. Püschel, M. Röglinger, H. Schlott, What's in a smart thing? Development of a multi-layer taxonomy, in: International Conference on Information Systems (ICIS 2016), 2016.
[32] L. Barker, M. White, M. Curran, Z. Patoli, B. Huggins, T. Pascu, N. Beloff, Taxonomy for Internet of Things-Tools for Monitoring Personal Effects, in: PECCS, 2014, pp. 67–71.
[33] S. Muralidharan, A. Roy, N. Saxena, MDP-IoT: MDP based interest forwarding for heterogeneous traffic in IoT-NDN environment, Future Gener. Comput. Syst. 79 (2018) 892–908.
[34] A. Ouaddah, H. Mousannif, A.A. Elkalam, A.A. Ouahman, Access control in the internet of things: big challenges and new opportunities, Comput. Netw. 112 (2017) 237–262.
[35] D. Midi, Security Techniques for Sensor Systems and the Internet of Things, Ph.D. thesis, Purdue University.
[36] S. Yablonsky, Smart wearable multi-sided fashion product platforms, in: Workshop on Business Models and ICT Technologies for the Fashion Supply Chain, Springer, 2016, pp. 135–150.
[37] P. Kale, V. Shinde, Framework and feature equivalence study of localization techniques for WSN, Int. J. Innovat. Eng. Res. Technol. (2016).
[38] S. Banerjee, T. Hemphill, P. Longstreet, Wearable devices and healthcare: data sharing and privacy, Inf. Soc. 34 (1) (2018) 49–57.
[39] S. Bhatt, F. Patwa, R. Sandhu, An access control framework for cloud-enabled wearable internet of things, in: Collaboration and Internet Computing (CIC), 2017 IEEE 3rd International Conference on, IEEE, 2017, pp. 328–338.
[40] A. Taivalsaari, T. Mikkonen, A taxonomy of IoT client architectures, IEEE Softw. 35 (3) (2018) 83–88.
[41] B. Alsamani, H. Lahza, A Taxonomy of IoT: Security and Privacy threats, in: Information and Computer Technologies (ICICT), 2018 International Conference on, IEEE, 2018, pp. 72–77.
[42] H. Boyes, B. Hallaq, J. Cunningham, T. Watson, The industrial internet of things (IIot): an analysis framework, Comput. Ind. 101 (2018) 1–12.
[43] R.E. Mohamed, A.I. Saleh, M. Abdelrazzak, A.S. Samra, Survey on wireless sensor network applications and energy efficient routing protocols, Wirel. Pers. Commun. 101 (2) (2018) 1019–1055.
[44] H. Sundmaeker, P. Guillemin, P. Friess, S. Woelfflé, Vision and challenges for realising the internet of things, Cluster Eur. Res. Project. Internet Things Eur. Comm. 3 (3) (2010) 34–36.
[45] M.K. Masten, Electronics: the intelligence in intelligent control, IFAC Proc. Vol. 30 (7) (1997) 1–11.
[46] K.M. Basher, J.-I. Nieto-Hipolito, M.D.L.A.C. Leon, M. Vazquez-Briseno, J.d.D.S. López, R.B. Mariscal, Major existing classification matrices and future directions for internet of things, Adv. Internet Thing. 7 (04) (2017) 112.
[47] L. Da Xu, W. He, S. Li, Internet of things in industries: A Survey, IEEE Trans. Ind. Inf. 10 (4) (2014) 2233–2243.
[48] C. Bormann, M. Ersue, A. Keranen, Terminology for Constrained-Node Networks, Technical Report, 2014.
[49] H. Jayakumar, A. Raha, Y. Kim, S. Sutar, W.S. Lee, V. Raghunathan, Energy-efficient dystem design for IoT devices, in: Design Automation Conference (ASP-DAC), 2016 21st Asia and South Pacific, IEEE, 2016, pp. 298–301.
[50] H. Jayakumar, K. Lee, W.S. Lee, A. Raha, Y. Kim, V. Raghunathan, Powering the internet of things, in: Proceedings of the 2014 International Symposium on Low power Electronics and Design, ACM, 2014, pp. 375–380.
[51] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of things (IoT): a Vision, architectural elements, and future directions, Future Gener. Comput. Syst. 29 (7) (2013) 1645–1660.
[52] A. Al-Fuqaha, A. Khreishah, M. Guizani, A. Rayes, M. Mohammadi, Toward better horizontal integration among IoT services, IEEE Commun. Mag. 53 (9) (2015) 72–79.
[53] N. Srinidhi, S.D. Kumar, R. Banu, Internet of things for neophytes: a survey, in: Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT), International Conference on, IEEE, 2017, pp. 234–242.
[54] R.K. Poluru, S. Naseera, A literature review on routing strategy in the internet of things, J. Eng. Sci. Technol. Rev. 10 (5) (2017).
[55] I. Mashal, O. Alsaryrah, T.-Y. Chung, C.-Z. Yang, W.-H. Kuo, D.P. Agrawal, Choices for interaction with things on internet and underlying issues, Ad Hoc Netw. 28 (2015) 68–90.
[56] L.F. Rahman, T. Ozcelebi, J.J. Lukkien, Choosing your IoT programming framework: architectural aspects, in: Future Internet of Things and Cloud (Fi-Cloud), 2016 IEEE 4th International Conference on, IEEE, 2016, pp. 293–300.
[57] R. Pozza, M. Nati, S. Georgoulas, K. Moessner, A. Gluhak, Neighbor discovery for opportunistic networking in internet of things scenarios: A Survey, IEEE Access 3 (2015) 1101–1131.
[58] P. Barker, M. Hammoudeh, A survey on low power network protocols for the internet of things and wireless sensor networks, in: Proceedings of the International Conference on Future Networks and Distributed Systems, ACM, 2017, p. 33.
[59] Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran, S. Guizani, Internet-of-things-based smart cities: recent advances and challenges, IEEE Commun. Mag. 55 (9) (2017) 16–24.

[60] V. Issarny, M. Caporuscio, N. Georgantas, A perspective on the future of middleware-based software engineering, in: Future of Software Engineering, FOSE'07, IEEE, 2007, pp. 244–258.
[61] S. Jha, R. Kumar, J.M. Chatterjee, M. Khari, et al., Collaborative handshaking approaches between internet of computing and internet of things towards a smart world: a review from 2009–2017, Telecommun. Syst. 1–18.
[62] H.-D. Ma, Internet of things: objectives and scientific challenges, J. Comput. Sci. Technol. 26 (6) (2011) 919–924.
[63] QinYongrui Louie, Managing Data Dynamics, Streams and Sharing in the Internet of Things, Ph.D. thesis, The University of Adelaide, 2015.
[64] E. Siow, T. Tiropanis, W. Hall, Analytics for the internet of things: a survey, ACM Comput. Surv. (CSUR) 51 (4) (2018) 74.
[65] M.J. Santofimia, D. Villa, F.J. Villanueva, S. Escolar, J.C. Lopez, A semantic middleware architecture for supporting real smartness, in: Industrial Electronics Society, IECON 2016-42nd Annual Conference, IEEE, 2016, pp. 6925–6930.
[66] S. Verma, Y. Kawamoto, Z. Fadlullah, H. Nishiyama, N. Kato, A survey on network methodologies for real-Time analytics of massive IoT data and open research issues, IEEE Commun. Surv. Tutor. 19 (3) (2017) 1457–1477.
[67] A. Karim, A. Siddiqa, Z. Safdar, M. Razzaq, S.A. Gillani, H. Tahir, S. Kiran, E. Ahmed, M. Imran, Big data management in participatory sensing: issues, trends and future directions, Future Gener. Comput. Syst. (2017).
[68] A. Heydarnoori, F. Mavaddat, Reliable deployment of component-based applications into distributed environments, in: Information Technology: New Generations, 2006. ITNG 2006. Third International Conference on, IEEE, 2006, pp. 52–57.
[69] R. Roman, J. Zhou, J. Lopez, On the features and challenges of security and privacy in distributed internet of things, Comput. Netw. 57 (10) (2013) 2266–2279.
[70] M. Stolikj, Building Blocks for the Internet of Things, Eindhoven University of Technology, Ph.D. thesis, 2015.
[71] D. Chasaki, C. Mansour, Security challenges in the internet of things, Int. J. Space-Based Situat. Comput. 5 (3) (2015) 141–149.
[72] T. Walter, L. Bussard, Y. Roudier, J. Haller, R. Kilian-Kehr, J. Posegga, P. Robinson, Secure mobile business applications–Framework, architecture and implementation, Inf. Secur. Tech. Rep. 9 (4) (2004) 6–21.
[73] E. Ahmed, I. Yaqoob, A. Gani, M. Imran, M. Guizani, Internet-of-things-based smart environments: state of the art, taxonomy, and open research challenges, IEEE Wirel. Commun. 23 (5) (2016) 10–16.
[74] P. Challa, B.E. Reddy, Content-centric global Id framework for naming and addressing for smart objects in IoT, in: Proceedings of the Second International Conference on Computational Intelligence and Informatics, Springer, 2018, pp. 153–162.
[75] H. Boujezza, A.-M. Modher, H.K.B. Ayed, L. Saidane, A Taxonomy of Identities Management Systems in IoT, in: Computer Systems and Applications (AICCSA), 2015 IEEE/ACS 12th International Conference of, IEEE, 2015, pp. 1–8.
[76] A. Chowdhury, S.A. Raut, A survey study on internet of things resource management, J. Netw. Comput. Appl. (2018).
[77] O. Eris, J. Drury, D. Ercolini, A collaboration-focused taxonomy of the internet of things, in: Internet of Things (WF-IoT), 2015 IEEE 2nd World Forum on, IEEE, 2015, pp. 29–34.
[78] J.D. Thompson, Organizations in action: social science bases of administrative theory, Routledge, 2017.
[79] S. Bhushan, B. Bohara, P. Kumar, V. Sharma, A new approach towards IoT by using health care-IoT and food distribution IoT, in: Advances in Computing, Communication, & Automation (ICACCA)(Fall), International Conference on, IEEE, 2016, pp. 1–7.
[80] E. Guillén, J. Sánchez, L.R. López, IoT protocol model on healthcare monitoring, in: VII Latin American Congress on Biomedical Engineering CLAIB 2016, Bucaramanga, Santander, Colombia, October 26th-28th, 2016, Springer, 2017, pp. 193–196.
[81] L.M. Borges, F.J. Velez, A.S. Lebres, Survey on the characterization and classification of wireless sensor network applications, IEEE Commun. Surv. Tutor. 16 (4) (2014) 1860–1890.
[82] X. Mountrouidou, B. Billings, L. Mejia-Ricart, Not just another internet of things taxonomy: a method for validation of taxonomies, Internet Things 6 (2019) 100049.
[83] M. Bauer, N. Bui, J. De Loof, C. Magerkurth, A. Nettsträter, J. Stefa, J.W. Walewski, IoT reference model, in: Enabling Things to Talk, Springer, 2013, pp. 113–162.
[84] P. Patel, D. Cassou, Enabling high-level application development for the internet of things, J. Syst. Softw. 103 (2015) 62–84.
[85] F. Ciccozzi, I. Crnkovic, D. Di Ruscio, I. Malavolta, P. Pelliccione, R. Spalazzese, Model-Driven engineering for mission-Critical IoT systems, IEEE Softw. 34 (1) (2017) 46–53.