IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 23, 2019, accepted January 13, 2020, date of publication January 27, 2020, date of current version February 5, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2969698

Graphical Framework for Categorizing Data Capabilities and Properties of Objects in the Internet of Things

JORGE EDUARDO IBARRA-ESQUER[1], (Member, IEEE), FÉLIX FERNANDO GONZÁLEZ-NAVARRO[2], J. SALVADOR SÁNCHEZ[3], (Senior Member, IEEE), BRENDA LETICIA FLORES-RÍOS[2], MARÍA ANGÉLICA ASTORGA-VARGAS[1], AND MARIA LUISA GONZÁLEZ-RAMÍREZ[1]

[1]Facultad de Ingeniería, Universidad Autónoma de Baja California, Mexicali 21280, México
[2]Instituto de Ingeniería, Universidad Autónoma de Baja California. Mexicali 21280, México
[3]Department of Computer Languages and Systems, Institute of New Imaging Technologies, Universitat Jaume I, 12071 Castelló de la Plana, Spain

Corresponding author: Félix Fernando González-Navarro (fernando.gonzalez@uabc.edu.mx)

This work was supported by the Universidad Autónoma de Baja California.

ABSTRACT Things are the core of the Internet of Things (IoT) and must be properly characterized according to the different functions they accomplish. Identifying their capabilities and combining them as sets provides a view on the single or joint properties of existing things and guide in properly designing and building new things while maximizing their potential benefits within an IoT system or application. Building on five essential but independent capabilities of things (Identification, Localization, Sensing, Actuation, and Processing), four categories or groups of things are defined. These groups comprise a particular view of the diversity of objects found in the IoT, as trackable, data, interactive, or smart objects. In this paper, a description of the aforementioned capabilities is presented, stating how each of the groups of objects includes them. Then, given that data are the most important assets for both organizations and individuals a further description of the data objects group is made, proposing a graphical categorization framework that thoroughly describes and measures the level in which each of these capabilities is contained and how it contributes to the performance and data properties of any data object.

INDEX TERMS Data objects, data properties, Internet of Things, things capabilities, categorization framework.

I. INTRODUCTION

The Internet of Things (IoT) has been regarded as one of the disruptive technologies of the 21st century [1]. Many definitions have been proposed for the IoT, but, in a general manner, it can be described as the confluence of several technologies that allow providing Internet-based services and applications supported by electronic devices attached to physical things for acquiring data and controlling processes [2].

The initial concern on the IoT was as a connection and communication point for physical objects able to obtain data from the environment but has recently changed to a more comprehensive approach where the focus is on the importance for organizations and individuals to gain access to those data and manage their connected objects for maximizing profits. Projections on billions of connected devices creating and obtaining enormous amounts of data and facilitating the automated control and monitoring of processes drive an enhanced interest on the establishment of the IoT as a productive technology for different sectors, including industry, academia, and society.

An architectural view of the IoT helps understanding how these technologies are arranged and organized to make such services and applications available to end-users, enabling access to data and the information derived from these data. Just as is the case with the visions and definitions of the IoT, there are several architectures and reference models for the IoT that have been proposed either by research and interest groups [3]–[5] or derived from industrial developments [6]–[12]. Even though these architectures and reference models usually reflect the interests of specific groups, companies or consortiums, some similarities might be found,

The associate editor coordinating the review of this manuscript and approving it for publication was Young Jin Chun.

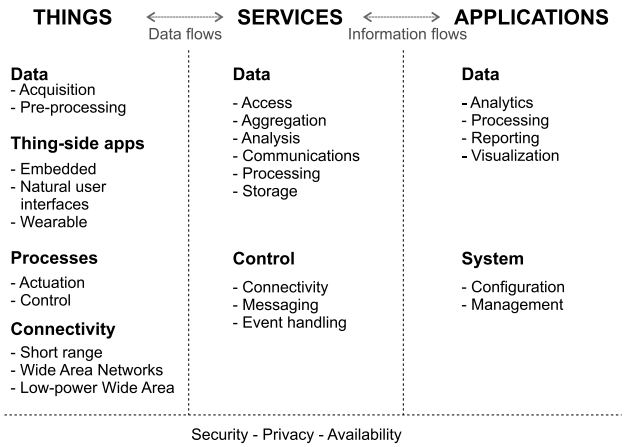

FIGURE 1. Abstraction of proposed IoT architectures and reference models.

observing that they are usually organized into three common sections or layers: Objects or Things, Services, and Applications (Fig. 1).

Things are on the physical side of the architecture and include a variety of physical elements [13]. Some things are digital objects that can be tracked through space and time and contain the data history related to the specific object they represent [14]; others are physical objects enhanced with small electronic devices allowing them to obtain data from the environment, process such data, temporarily store them, and send them to the Internet [15]–[17]. In some cases, they might act on the environment via embedded actuators, and there are objects that may also provide the user with ways to interact with an application, system, and even among different things [13]. Data obtained from such things are arguably the most important assets for organizations and individuals deploying IoT-based systems.

A thing must have networking capabilities to be a part of the IoT. Things may be designed with such capabilities and manufactured as Internet-ready objects; non-Internet-enabled objects can be equipped with additional networking hardware; or things being part of an IoT system can connect to the Internet indirectly via additional objects that act as proxies when connecting them directly is not necessary, advisable, or possible [2].

The middle section consists of services that are typically provided as cloud-based, where data are stored, processed, analyzed, aggregated, and means for accessing them are provided. While the different models and architectures consider software and hardware as important components of IoT, some of them imply a relevance of data-related services across the whole model [7], [9] or highlight the importance of the data flows between sections [10]. As implied in [18] and [19], new services are emerging and made available due to the increasing number of IoT connected devices and as the technology itself reaches a higher maturing stage. IoT applications performing complex data-intensive computations benefit the most from these services [18].

In the Applications section, we find the end-user apps, either computer or mobile device based. They provide means for data visualization, reporting, analytics, things management and configuration, sending commands for actuation on things-side, and controlling things and systems behavior [6], [8]–[12]. Applications allow users to interact with connected objects via services, taking advantage of enhanced data and information useful for decision making.

Between these sections there is a continuous exchange of data and information supported by a set of technologies that provide security, privacy, and availability to data, services, and applications. Things obtain data and act as providers for the services section, where data are processed and turned into usable information that users on the applications side can then transform into knowledge.

As both services and applications depend on the data and processes obtained and controlled on the things section, we consider important to properly characterize and describe things according to their capabilities and functions. This document presents a definition for groups of things based on such capabilities and elaborates on a framework for a specific group of things that are identified as Data Objects (DO).

One of the most comprehensive approaches on creating a framework for describing the components of the IoT was performed by the Cyber-Physical Systems Public Working Group (CPS PWG) [19]. Even though their aim is defining and shaping key characteristics of CPS, along with developing a shared understanding of CPS and its fundamental concepts and unique dimensions, the working group acknowledges an overlap between the CPS and IoT concepts, making this framework suitable also for IoT. Different scopes for the application of the framework are presented, from single devices to interconnected systems, having as a goal the description of interoperable architectures for systems of CPS by means of several concerns that are addressed by well-defined activities and artifacts within three views or facets, tied to specific application domains.

In [20] authors present a survey of 17 commercial frameworks and platforms designed for implementing and running applications in the IoT. They identify a framework as a set of guiding principles, standards, and protocols which enable the implementation of IoT applications, and find different framework categories as those aimed for home automation, Industrial Internet of Things, interoperability between applications, monitoring and managing connected devices, and others that target specific aspects of the IoT, or that are looking to provide supervision and guidance to the development of IoT technologies.

The framework we are describing offers insights for designers of IoT applications and systems, while being independent of the chosen platform or implementation framework and technologies. It focuses on the data activities and properties of the thing-side of the IoT, isolating the data aspects of data-producing things, and creating a graphical representation of their data properties and activities instead of listings of properties and activities. These graphs offer a quick

view of the data-related capabilities of things and provide a data-footprint for each thing that can also be scoped to a system level.

The rest of the document is organized as follows. The things capabilities and object groups are defined in Section 2. Data objects are discussed in Section 3. The categorization framework is described in Section 4. A discussion on the impact of capability levels on data properties is presented in Section 5. Two use scenarios of the applicability of the framework are shown in Section 6. A brief discussion on the use of the framework is presented in Section 7. Finally, conclusions are outlined in Section 8.

II. THINGS CAPABILITIES AND OBJECT GROUPS

The importance of things as a key element in the IoT is evidenced by most definitions and interpretations of the technology. Things, also referred as smart objects, smart devices, or simply objects [15]–[17], [21], are regarded to as any machine, device, application, computer, virtual or physical object communicating through the Internet, which can create, request, consume, forward or have access to digital information [22]. These objects are commonly defined in terms of their physical, computing, sensing, actuating, and communications properties and characteristics [16], [17].

In [2] we identified the properties of things that were more frequently listed in the literature, abstracting them into five capabilities besides the essential Internet connectivity. These capabilities (Identification (IC), Localization (LC), Sensing (SC), Actuation (AC), and Processing (PC)) allow categorizing objects in the IoT according to what they can perform. Table 1 shows the description for the highest level of deployment of these capabilities, including some examples for each case. The first three capabilities {IC, LC, SC} refer to objects creating and providing data; {AC} is for objects that can act on the environment in response to collected data or instructions received from the Internet; the last one {PC} corresponds to a capability of transforming data that was obtained by the object using its sensors, or received from the Internet.

The Identification Capability (IC) refers to the identity of the thing. As implied before, there are different levels of identification, which might be associated with the specific needs of an IoT system or application or restricted by the available technologies for its implementation. In addition, IC can range from the complete object or system seen as a thing in the IoT (e.g. a car, a tree, or even a person) to the particular device enabling the object to become a part of the IoT (e.g. a microcontroller, a smart sensor, or an electronic tag). Initial IoT visions were based on the concept of being able to electronically tag and identify any object, anywhere at any time without the need of human intervention, linking them to the global Internet [23], [24].

A thing that needs to be located within a certain geographical space should implement LC. This capability is also important when objects are not fixed to a physical location and need to be tracked while they are moving from one place to another.

TABLE 1. Things capabilities.

Capability	Description	Typical implementation
IC	Being uniquely and unmistakably identified.	Electronic tags, hard-coded serial numbers, or printed labels that are read by other objects.
LC	Being able to know their precise physical location in the world by their own means.	Embedded geolocation devices.
SC	Obtaining data from the environment or their actual state.	Sensors for different physical parameters or variables (e.g. temperature, pressure, acceleration).
AC	Acting on the environment, modifying its parameters.	Actuators for controlling systems (e.g. motors, valves, solenoids).
PC	Processing data obtained by them or received via the Internet.	Embedded processors or programmable devices.

An object with sensing capabilities (SC) can obtain one or several types of physical data and transmit it through an Internet connection, either raw or pre-processed if the object also has processing capabilities (PC) that allow selecting or transforming data. Sensed data may range from simple measures like temperature or pressure, to more complex representations of physical phenomena as sound, pictures, or even video which are provided to an IoT system as either structured or unstructured data. Data can also be obtained from the object itself, i.e. battery level, internal temperature, current task progress, or whether a certain object is turned on or off. Therefore, SC refers to an object ability to sense data from their environment, measure internal properties, or both.

Finally, the Actuation Capability (AC) is essential for things that modify properties of their surrounding environment or control processes as part of an IoT system. This capability is typically implemented by means of actuation devices as motors or valves and heavily used in IoT-based automation applications and systems.

To be included as part of the IoT a thing must implement at least one of {IC, LC, SC, AC}, as represented in the shaded area of the Euler diagram in Fig. 2. While PC enhances any of the other capabilities, it does not provide a computational device with characteristics that differentiate it from a general-purpose computer, thus a device that only has this capability but none of the others is not seen as a thing in the IoT. Capabilities can be combined in several ways depending on the requirements of the IoT application they are designed for, shaping different types of objects according to each subset of capabilities [2]. The connectivity requirement may be a part of the object or provided by an additional object acting as a gateway. This is the case for the original

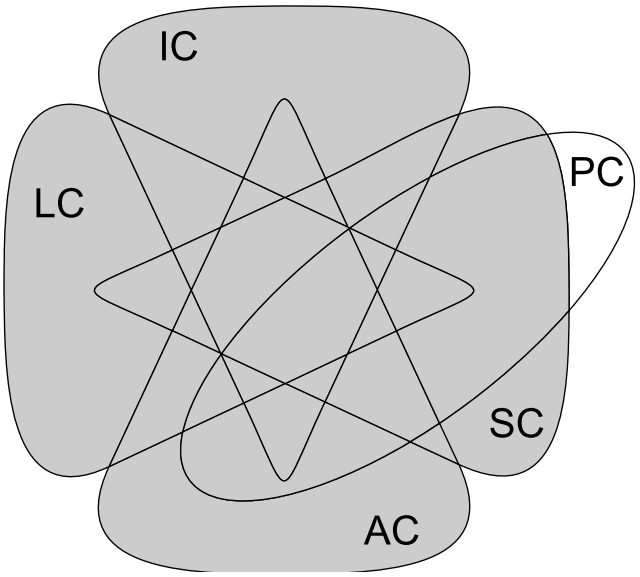

FIGURE 2. Visualization of the capabilities of things in the IoT as sets [2].

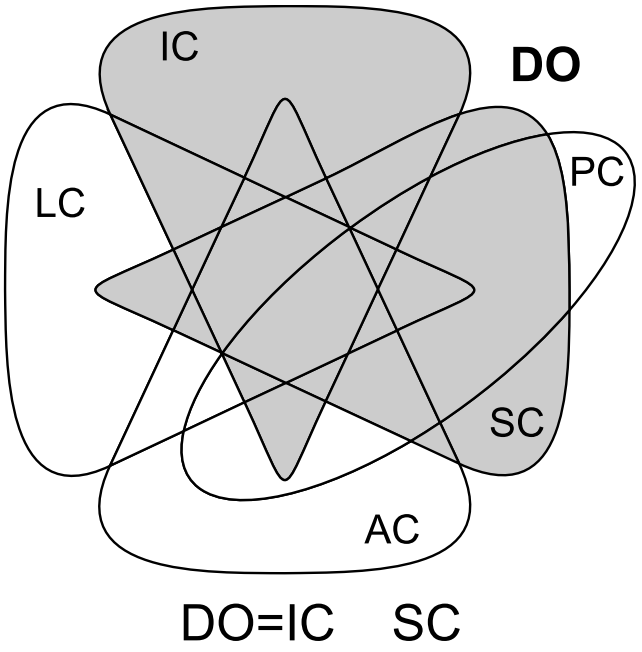

FIGURE 3. DO are things in the IoT with Identification or Sensing capabilities [2].

things that the IoT was devised to integrate, i.e. electronic tags attached to objects, that would be read by another object allowing to identify them at any time and communicate data through the Internet [23], [25], also referred as Tagged Things and deemed as the first generation of IoT solutions [26], and more recently exploited by the use of fog computing platforms [27].

As described in a non-exhaustive manner in [2], different combinations of capabilities result in several subsets for things in the IoT. One of such is what we identified as DO whose characteristics are thoroughly described in the next section.

III. DATA OBJECTS

DO consist of any object that has either identification or sensing capabilities, or both, as shown in the shaded area of Fig. 3. These objects can get data from the environment by means of embedded or attached sensors, or internal data from their current state, properties or identity.

DO can produce data either from sensors, their current properties or state, or provide some type of data that allows identifying the object [2]. The first two cases indicate obtaining variable data, while the latter is about constant values that may be specific to the object, useful for identifying it from related registries stored in cloud repositories and accessible to applications.

Implementing SC allows a DO to obtain variable data through sensors. These are devices needed to measure signals and parameters of an engineering system and its environment [28], forming the front end of the IoT devices [29]. Equipping a physical object with sensors allows the object to interact with the environment as a human does by means of the five senses. In addition, the object properties or state refer to internal parameters of the object.

The other capability of DO is IC. The identity of the thing is the most basic type of data that can be obtained. This is a set of constant values leading to different levels of identification of an object (e.g. type or class of object, brand, model, serial number).

As additional capabilities are added to a DO and as these are deployed at a higher level, things become more complex and so does the type of data that can be obtained from them. For instance, if the location capability (LC) is added to an already identifiable object (i.e., the intersection of IC and LC) makes what we have called Trackable Objects (TO). TO are mobile things that can be identified and are aware of their physical location [2]. In other words, TO are DO that can go from one place to another and be identified and physically located by a requesting IoT service or application. Even though location of a thing is actually data being measured by a location sensor, objects that only produce this type of data were not included as part of the DO set, as it would indicate the existence of an object at a specified physical location, but no extra information could be inferred and used, or actions be taken on the object. The capability is presented separate from SC, as the type of data measured is very specific to the location of an object, while in SC the number of sensors and type of physical parameters that can be read are numerous and can grow as new types of sensors are created.

By inspecting the diagram in Fig. 3, there are 22 possible combinations or subsets of capabilities within the DO set. TO subset is one of them, but they can range from the simple identifiable objects to fully interactive and data

processing smart objects. However, two objects possessing a given capability not necessarily are capable of sensing, processing and providing the same type of data, as technical restrictions, or even the needs of the system or application where each object is embedded require different levels of deployment for each capability. Thus, categorizing and describing a DO is not just dependent on the capabilities the object possesses, but also on the extent that each capability is used by the object.

The diagram in Fig. 3 also shows that some data objects can have AC in addition to their data collection, creation, and transformation capabilities. However, as AC does not directly provide, create, or act on the data provided by the object, it is not included in any further description or discussion about DO, even though some DO may have the capability of acting on the environment.

Taking this into account, we propose a categorizing framework for DO based on the level of deployment of their capabilities, which is described in the next section. This framework is mostly of a graphical nature, allowing the creation of data footprints for objects in the IoT that provide designers and users a descriptive view of the type and volume of data a DO provides per unit of time. Additional constraints should be considered when involving time, as the processing and measuring limits of the object and each of its sensors, as well as the requirements of the IoT application and the capacities of the network result in different types of data streams that must be either processed or transmitted to a cloud service following approaches suitable for real-time and time-critical systems as the ones described in [30], [31]. These considerations are currently beyond the scope of the framework but will be incorporated after a thorough validation is made.

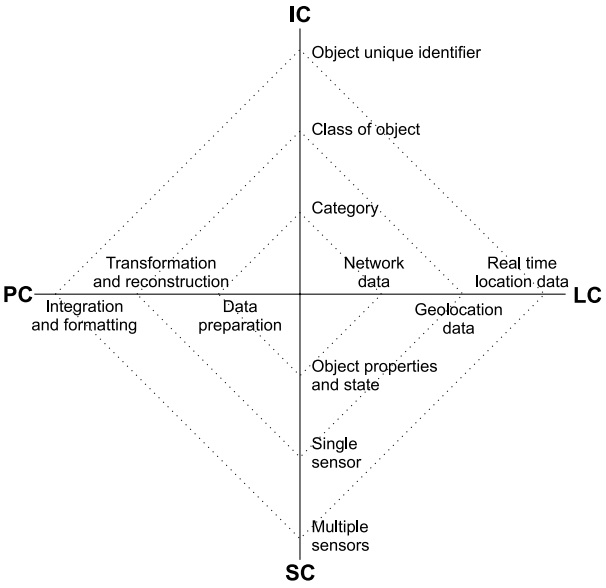

FIGURE 4. Characteristics of data provided by DO according to the level of each capability.

TABLE 2. Levels of deployment for identification capability (IC).

Level	Description	Examples
Basic	A general category of the object.	A motor vehicle.
Intermediate	The specific class or type of object.	Sedan, SUV, Crossover.
Advanced	A unique identifier leading to the precise identification of the object.	Vehicle serial number or license plate.

IV. CATEGORIZATION FRAMEWORK FOR DATA OBJECTS

Identifying the subset of capabilities of any single DO provides a high-level description of the object and a basic view of what can be attained by the object itself as well as its functional contributions in the context of an IoT system [32]. For instance, stating that a DO has SC indicates it is able to measure one or more parameters from the environment, either internal or external, but does not provide any details on the specific type of data the object can sense and provide, and the same situation applies for any of the data producing capabilities {IC, LC, SC, PC}. To create a richer description and understanding of the DO, we propose a graphical categorization framework that provides an extended representation showing the level of implementation for each capability and their individual and collective effects on the object's contributions to an IoT system in terms of data.

The graphical categorization framework for DO consists of a qualitative 4-axis radar chart, with three discrete levels for each of the axes. One axis is used for each of the data-producing capabilities in a DO with three data-related features for measuring these capabilities. Fig. 4 presents a general view of the features and defines a first level of identification of data and data activities in DO. This chart is completed by measuring or specifying each capability individually from the specific activities or properties they provide to the object and then arranging them to create a unified view of a DO and a more precise specification of the data that can be acquired from it.

On the IC axis, three levels of identification are proposed for an object as category, type or class, and unique ID, being the latest the most precise and including the previous levels. A brief description and examples of identification are presented in Table 2. Either IC or SC are required capabilities for DO, with the simplest DO having only a basic level of identification indicating an object's presence in the Internet, like a beacon; non-identifiable DO are also a possibility for IoT systems that gather sensor data but do not need to identify the source, or the identity is implicit in the system.

Likewise, three levels are defined for the LC axis according to the type of data the object can provide in order to know its precise location. Different from identification data, location data are dependent on different conditions from the environment, location technology, characteristics of the object, and needs of the IoT system that impact on its accuracy and volume. A description of the levels is presented in Table 3, along with examples of typical implementations.

TABLE 3. Levels of deployment for localization capability (LC).

Level	Description	Typical implementation
Basic	Approximate location of the object. Useful for IoT systems were the objects tend to remain in the same location and precise location is either not needed or can be inferred from additional data related to or measured by the specific object.	Passive location obtained from network parameters.
Intermediate	Geolocation data provided by the object when network connections are available for analyzing and processing the data. Suitable when real time location is not mandatory in the IoT system.	Assisted-GNSS and Cloud-GNSS positioning technologies.
Advanced	Real time location data obtained and provided by the object. Needed when keeping track of the object location and position related parameters is important for the IoT system.	GNSS receivers incorporated into the devices.

TABLE 4. Levels of deployment for sensing capability (SC).

Level	Description	Examples
Basic	Data created or measured inside the object.	Internal sensors providing data to monitor the state of the object and parameters as battery level, energy consumption, or temperature of the object.
Intermediate	A single external parameter measured by a sensor.	Data from any physical phenomena of the environment where the DO is located.
Advanced	Multiple external parameters measured by sensors.	Multivariate data from physical phenomena of the environment where the DO is located.

TABLE 5. Levels of deployment for processing capability (PC).

Level	Description	Common data activities
Basic	Objects execute data cleaning and selection algorithms.	Noise, duplicates, or outlier detection and removal.
Intermediate	Objects can transform and reconstruct data obtained by sensors.	Create new data from measured values or reconstruct missing data.
Advanced	Objects perform data integration and formatting.	Combine values from multiple sensors and create the datasets needed by the IoT system.

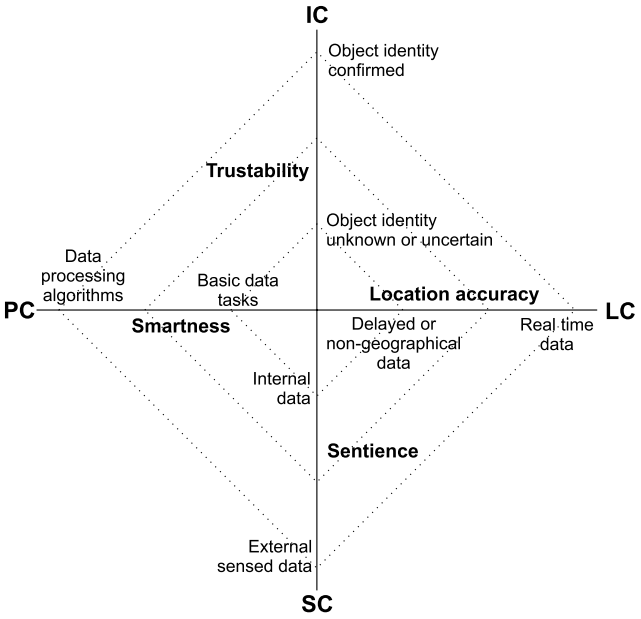

FIGURE 5. Contribution of each capability to data properties in DO.

Most accurate technologies for location are based on Global Navigation Satellite System (GNSS), being the Global Positioning System (GPS) the most common implementation of them. An extensive description and analysis of location technologies is presented in [33].

The SC axis helps in characterizing the type and amount of data provided by the object (Table 4). A DO with SC constitutes the basic element for an IoT system that monitors conditions on the physical side of the system: a DO can provide internal data like its current properties or state, external data obtained with a single sensor, or contain multiple sensors that collect several types of data.

The PC axis states what a DO is capable of doing with the data before sending it to the Internet, ranging from data cleaning to integration and formatting (Table 5). If a DO does not have PC it will send raw data to the IoT system. Most advanced data activities might combine data obtained from multiple sensors or even from multiple DO to create ready-to-use datasets that will be provided to the services layer for processing. The goal of having PC in a DO is to increase the ratio of usable data that are sent to the IoT system. Data compression algorithms can also aid in reducing the volume of data transmitted, at expenses of more processing power and latency in transmission of data.

The technology requirements for constructing new things are closely related to the data they are aimed to create or obtain; the type and characteristics of these data can be inferred from the visualizations created by identifying or defining the level of deployment for each capability in a DO and tracing them on a chart. Furthermore, this level has an impact on data properties that should be taken into account as it also influences the performance of an IoT system. The following section complements the description of the framework by elaborating on the effects that capability levels have on data properties.

V. IMPACT OF CAPABILITY LEVELS ON DATA PROPERTIES

A more detailed view of the level of contribution of each capability is presented in Fig. 5. Every axis is labeled according to a data-related property of the object that is improved as the level of contribution of that capability increases, along with

TABLE 6. Capability impact on data properties.

Capability	Quality	Volume	Confidence
IC	Very low	Very low	Very high
LC	Very low	High	Low
SC	Low	Very high	None
PC	Very high	Low	Low

a general description of the types of data the object can provide. In addition, and as a result of those contributions, each capability impacts on a different level the quality, volume and confidence of generated data (Table 6).

A higher level in the IC axis implies an increased trustability on the data and the object itself. In other words, as more certain an IoT system is on a data provider's identity, there is a higher confidence in both the data and the system performance. Trusting the provider and the data is of special importance when an IoT system contains several DO and data-derived decisions are important not only at system-level but also as individual or node-level. An example of the first type is the air pollution monitoring and forecasting system presented in [34], where data from all the sensors in the system are used to feed a neural network. In [35] a similar system is described, but data are processed and results displayed to users for each of the monitoring nodes, making it necessary for the system to uniquely identify each node.

Moving ahead in the LC axis accounts for better location accuracy of an object. At the lowest level, objects that are not permanently connected to the Internet can be located using their last location reported or within the coverage area of a local network. An object able to provide geographical data can be located within the availability and accuracy of GPS. A higher rate of positioning data leads toward real time location of the DO, which is important when objects change location continuously, with the drawback that the amount of data generated grows as the update frequency increases.

The SC axis describes the sentience of the DO with respect to its surrounding environment. A non-sentient object will only provide internally generated data that help monitoring the object's state and performance-related parameters. As sensors are added to an object it becomes sentient of the environment, being able to measure its properties and gather data. With more sensors, multiple properties can be measured, making the object more sentient of different types of data and increasing the volume of collected data.

The PC axis defines the smartness of a DO as it provides the object with means to act on received or collected data. Smartness increases as the object advances from executing basic data tasks to complex data processing algorithms, though this implies more resources needed for processing. As the devices embedded on physical things are usually resource constrained and typically running on batteries, it is advisable to limit the data processing to basic tasks and relying on edge, fog, or cloud processing for more complex activities.

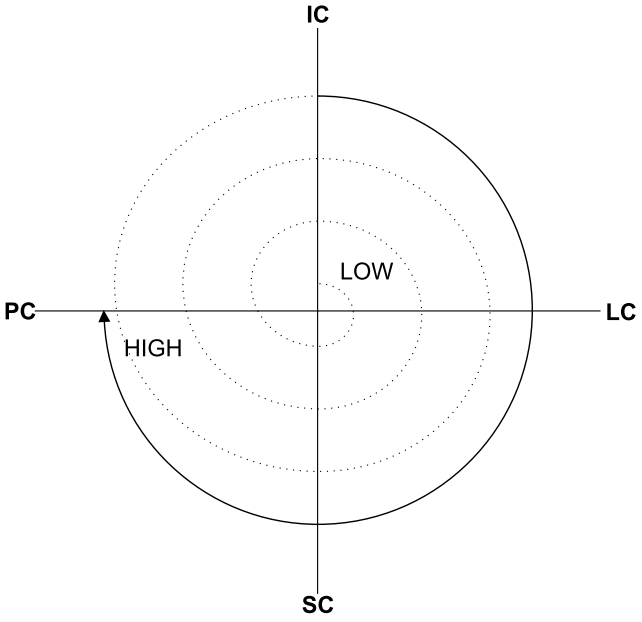

FIGURE 6. Complexity of a DO increases as more properties are added to each capability. PC properties are the most complex among the four capabilities in this type of objects.

However, with smaller, energy-efficient and more powerful devices being developed and made available for the IoT, DO will be able to execute that type of activities and create better data.

Based on this framework, it is possible to categorize any existing DO in the IoT and establish a general notion of the complexity of these and new objects from early design stages of an IoT system. This complexity can be observed graphically by moving clockwise in the chart, starting from the IC axis, i.e. IC properties are less complex to include on a DO than PC properties (Fig. 6), as an electronic tag is enough to identify the object, but in order to clean or filter data the object needs an embedded processor and memory resources. Following this same path but also moving up gradually on each of the axis would describe a spiral of complexity for DO, with more complete, capable, and complex objects away from the origin of the chart.

Summing up the previously discussed considerations, several categories for DO are realizable as the combination of deployment of capability levels and their combined contribution to data quality, volume, and confidence allows. General categories could be set as Data intensive objects, Trusted objects, and Ready-to-use data objects (Fig. 7), by taking the description of capabilities impact on data. These categories can be joint when a DO incorporates high levels of deployment of its capabilities that would cover more than one category, and sub-categories could also be defined based on lower levels of deployment.

Rather than providing a comprehensive listing of categories, the recommendation is to use the framework in a graphical manner, categorizing the DO according to the shaded area in the radar chart. Objects belonging to any of

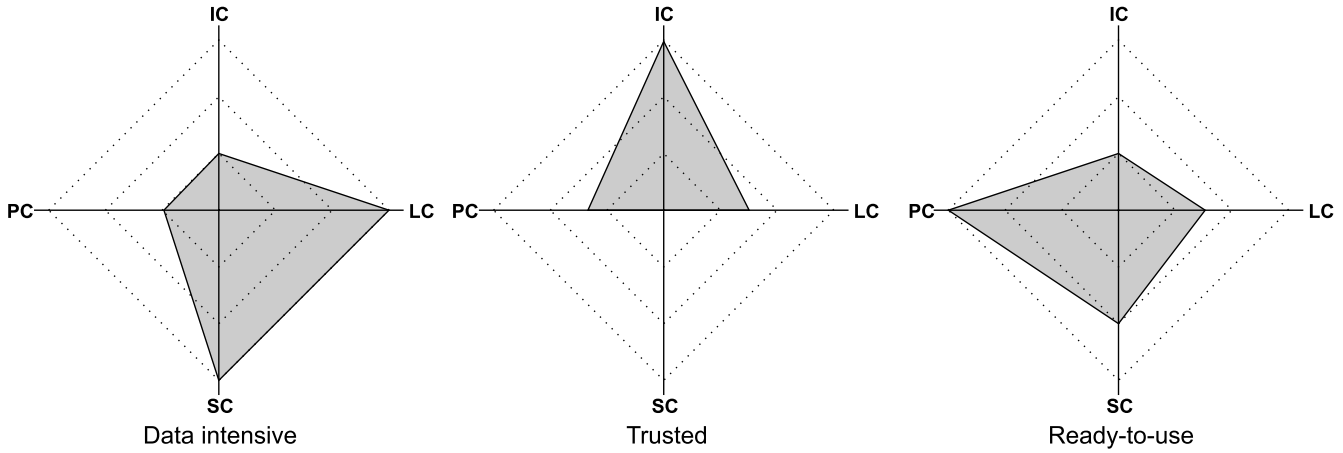

FIGURE 7. Areas covered by data objects categorized as Data intensive, Trusted, and Ready-to-use.

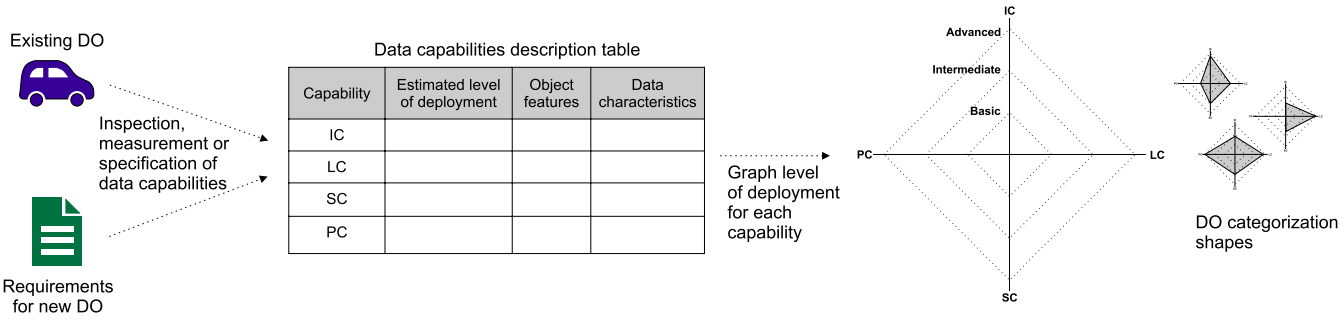

FIGURE 8. Suggested use of the framework. Data capabilities are extracted to a description table and then graphed into the radar chart to create the categorization shape.

the proposed categories would cover the shaded areas shown in the charts of Fig. 7. High levels of SC and LC are present in Data intensive objects which are common in personal health devices or environmental monitors; IC is high while LC and PC can range from medium to low levels in Trusted objects, as usually observed in security devices; Ready-to-use DO have strong PC with mid to high levels of SC and LC, as found in devices that integrate some type of biometric recognition or authentication.

VI. APPLICABILITY OF THE FRAMEWORK

The applicability of the framework is exemplified with a fictitious vehicle-related scenario and the characterization of an existing commercial IoT air quality monitor [36]. In both cases the radar charts specify the level of implementation of each capability and an assessment on the DO categories is inferred from the resulting shape.

To create these shapes either the documentation of an existing DO, the object itself if documentation is not available, or the requirements for a new DO are examined to extract the characteristics of their data capabilities. According to these characteristics and the object features, the level of deployment of each of its capabilities is classified as Basic, Intermediate, or Advanced, using as a reference the levels described in Tables 2 to 5. A Data Capabilities Description Table is proposed as an aid in recording the estimated or required level of implementation for each capability. The assigned levels are then graphed into a radar chart, obtaining a categorization shape for the DO. Fig. 8 outlines the suggested steps to create the categorization shapes from the areas covered in the radar graph.

A description of a mid-complexity DO with high data volume generation and class-level identification is presented by means of a scenario where several vehicles provide temperature readings and report their locations in real time as part of an IoT system. In the system, vehicles would act as the things providing data, or data objects, equipped with sensors for location and temperature, and an embedded processor for basic data tasks. The specific example shows the vehicle identified by its type, providing real time positioning data and temperature recorded by the sensor. The embedded processor performs outlier detection and removal on the sensor data, improving the quality of the data and limiting the transmission of unusable data.

In this case, the framework is used to categorize things at object-level, i.e. vehicles as DO independent of the contribution that multiple objects have as a system. From the description or requirements of the system, a summary of

TABLE 7. Categorization for automotive DO.

Capability	Estimated level of deployment	Object features	Data characteristics
IC	Intermediate	Vehicle identified by type.	Class of object.
LC	Advanced	Reported in real-time.	Real time location data.
SC	Intermediate	Temperature sensor.	Single sensor.
PC	Basic	Outlier detection and removal on data measured by the sensor.	Data cleaning and selection.

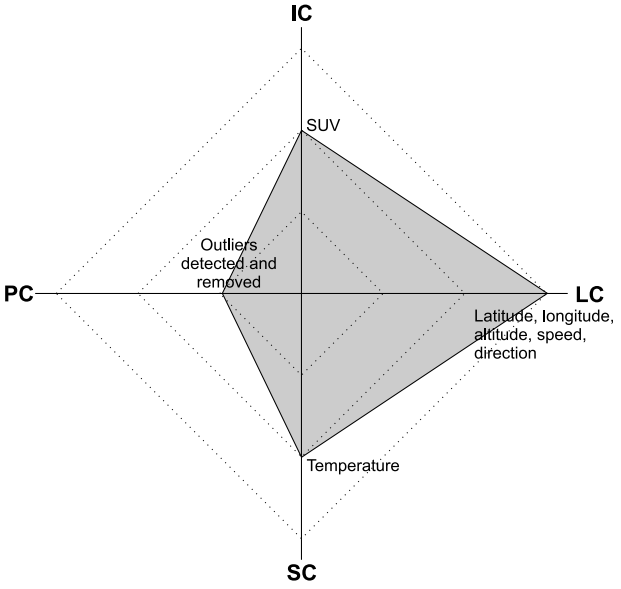

FIGURE 9. A scenario of the framework for an automotive DO.

the categorization criteria is extracted and recorded into the description table by making an estimate of the projected implementation of each capability in the DO (Table 7). Next, the chart shown in Fig. 4 is completed by placing a mark on each axis indicating the implementation level, and then joining the marks to create the shape. The shaded area in the chart of Fig. 9 covers a large portion of the suggested area for a data intensive object and also has elements to provide a high degree of confidence to the data in the ways a Trusted object is proposed (Fig. 7).

As stated before, the framework can be used to categorize existing IoT objects. To illustrate this feature, we selected an IoT device for the smart homes market and, by means of the properties and capabilities listed by the manufacturer [36] summarized in terms of capabilities in Table 8, obtained the shaded area shown in Fig. 10. This chart belongs to a Bitfinder Awair air quality monitor, which is a device that senses temperature, humidity, CO_2, chemicals, and small dust particles (PM2) present in the air, providing the user with a real time view of air quality in the area where the device is located. The monitor has direct Internet connection via WiFi and is linked to a user account and identified by a name

TABLE 8. Categorization data for the awair air quality monitor.

Capability	Estimated level of deployment	Object features	Data characteristics
IC	Advanced	The monitor is identified by an ID and a user-assigned name.	Object unique identifier.
LC	Basic	Services collect network data to infer location.	Network data.
SC	Advanced	Temperature, humidity, CO2, chemicals, and small dust particles (PM2) sensors.	Multiple sensors.
PC	Intermediate	Outlier detection and removal on data measured by the sensor.	Data transformation.

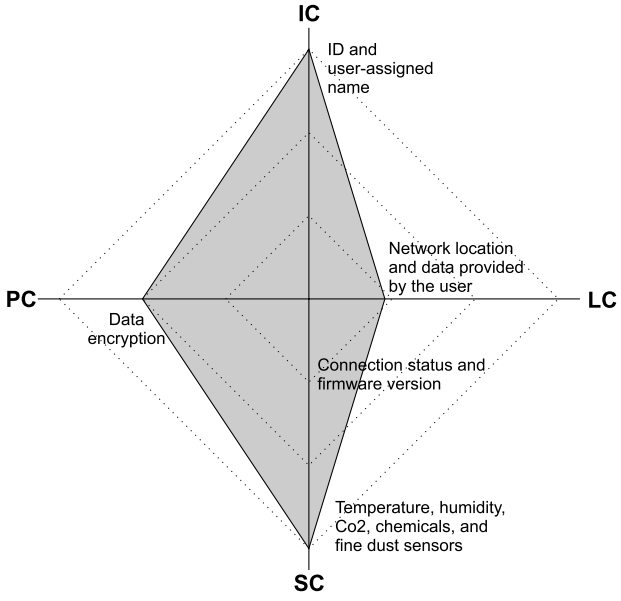

FIGURE 10. Categorization for the Bitfinder Awair air quality monitor.

assigned by the user; the Awair cloud services collect network data to provide location-specific insights on the environment, while specific indoors location data is provided by the user at setup-time. A proprietary app is used to setup the device, user preferences, and to connect to the cloud services in order to see historical data and suggest the user with air quality improvement actions based on collected data.

The resulting chart covers the areas proposed for trusted and data intensive objects. The device can be identified as a mid to high complexity DO as it obtains several types of data and performs transformation tasks on the data to increase privacy and security. In addition, the monitor has actuation capabilities to generate a visual feedback to the user and push notifications that are received and shown by the app.

VII. DISCUSSION

The framework was applied to a pair of IoT devices, one of them in a fictitious system and the other a commercial IoT air quality monitor. By means of these examples the procedure for using the framework is presented, and an interpretation of the resulting shapes in terms of complexity is also provided.

One of the main benefits of this framework is that its graphical nature allows to easily read the level of deployment of each capability within a DO, categorize it from the combination of such levels, and infer the complexity of the object. Once the Data Capability Description Table is completed, creating the graphs is also a streamline process, given that the information of the objects is available or can be obtained. For new objects this information should be part of requirement specification and design documents, but for existing objects has to be extracted and inferred from technical documents, user manuals, support forums, or websites.

The scope of application and expected use is different for both cases. Categorizing and characterizing a DO in terms of data since early design stages may guide in the selection of hardware and software tools and platforms that best fit the object and the system containing it. For existing objects, it delivers an outline of the data and types of data created by the object that, besides categorization, can be used for evaluating its performance, or to compare and aid in choosing between devices for a specific application from a data perspective. Several categories can be proposed for DO, but the recommendation is to adhere to the graphical nature of the framework and use the shaded areas in radar charts to visualize and infer object properties from a few general categories.

The framework is independent on the specific technologies and application domains. A slight exception is the LC axis, which is described around network and GPS location technologies that are the most widespread among GNSS technologies. However, technologies where recent and future advances have been achieved, especially in indoor location, may be effortlessly swapped into the framework. In addition, the number of levels in each axis can be modified, providing flexibility to the framework in order to adapt to specific needs of an IoT system, creating more detailed views of the DO structure, features, and properties.

VIII. CONCLUSION AND FUTURE WORK

The things-side is the part of the IoT that draws the main attention, as there is where objects are identified and tracked, data is collected, processes controlled, and the main expected benefits observed. Regardless of the size of the projected system or application, understanding the Things component of an IoT architecture provides clear insights on the type of devices, communication protocols, data-related tools and techniques, as well as how both user and thing-side applications would allow interaction with the whole IoT system.

Using sets of capabilities to describe different types of things or objects results in visual representations that offer a quick glimpse of the actions an object can perform and the types of data it can provide. One of the sets we find of bigger relevance is Data Objects (DO), given that it assembles capabilities that enable objects to gather data either from the environment or the object itself and send it to cloud-based services for processing, storage, and made available to end-user apps.

These capabilities can be deployed at different levels, describing data objects with common characteristics that we categorize by means of a graphical framework, setting a four-axis radar chart where each axis is assigned to one of the data-related capabilities. A capability-contribution diagram helped with observing how each capability contributes to enhance a DO trustability, location accuracy, sentience, and smartness. This diagram also allows to observe and infer the technological needs and requirements of the DO. Capabilities also impact data properties like quality, volume, and confidence, that are important parameters for the IoT system containing the DO.

When capabilities are seen as a whole, they have a combined effect on the DO and its data in both a qualitative and quantitative way. The framework aids in visualizing and describing this effect, along with the general properties of data provided by a DO, and the complexity for realizing the object.

The framework has the capability of allowing IoT solution designers and providers understand the scope and outcomes of both IoT products and projects. It can be used to categorize both existing objects and new objects before they are constructed, which is where designers would benefit most from it.

Further validation of the framework is needed and will be performed by identifying and choosing a representative set of existing DO in the IoT to obtain their categorization shapes. Iterating on this process with different DO will confirm the universality of the framework or guide in making adjustments to include missing features. Once fully validation is achieved, time-related properties can be incorporated to produce dynamic views of how a DO provides and processes data, which will result in enhanced representations of the capabilities of the DO. In addition, we consider important to model how data provided by DO flows through the sections or layers of the IoT in order to create information and knowledge. Finally, establishment of quantitative measures and scales to relate the level of implementation of data-related capabilities in a DO to its complexity, is in an early stage of development.

ACKNOWLEDGMENT

This work has been performed as part of project 105/6/C/25/4 at Universidad Autónoma de Baja California.

REFERENCES

[1] H. Alkhatib, P. Faraboschi, E. Frachtenberg, H. Kasahara, D. Lange, P. Laplante, A. Merchant, D. Milocijic, and K. Schwan, "What will 2022 look like? The IEEE CS 2022 report," *Computer*, vol. 48, no. 3, pp. 68–76, Mar. 2015, doi: 10.1109/MC.2015.92.

[2] J. E. Ibarra-Esquer, F. González-Navarro, B. Flores-Rios, L. Burtseva, and M. A. Astorga-Vargas, "Tracking the evolution of the Internet of Things concept across different application domains," *Sensors*, vol. 17, no. 6, p. 1379, Jun. 2017, doi: 10.3390/s17061379.

[3] C. Partnership, "Final report: RFID and the inclusive model for the Internet of Things," Eur. Commission, London, U.K., Tech. Rep. EU Project 216803, 2009.
[4] M. Bauer, M. Boussard, N. Bui, F. Carrez, C. Jardak, J. D. Loof, C. Magerkurth, S. Meissner, A. Nettsträter, A. Olivereau, M. Thoma, W. Joachim, J. Stefa, and A. Salinas, "Internet of Things—Architecture IoT-a deliverable D1.5—Final architectural reference model for the IoT v3.0," Eur. Commission, Univ. Surrey, Guildford, U.K., Tech. Rep. D1.5, Jul. 2013. [Online]. Available: http://bit.ly/IOTAD15
[5] A. Rayes and S. Salam, "Internet of Things (IoT) overview," in *Internet of Things From Hype to Reality*, 1st ed. Cham, Switzerland: Springer, 2017, ch. 1, pp. 1–34, doi: 10.1007/978-3-319-99516-8_1.
[6] Cisco, "The Internet of Things reference model," Cisco, San Jose, CA, USA, White Paper, 2014.
[7] Cisco. (2019). *Cisco IoT Solutions | Internet of Things services*. Accessed: Jan. 28, 2019. [Online]. Available: https://www.cisco.com/c/en/us/solutions/internet-of-things/overview.html
[8] Samsung. (2019). *Samsung ARTIK Platform Overview*. Accessed: Jan. 28, 2019. [Online]. Available: http://static.artik.io/files/Samsung_ARTIK_Overview.pdf
[9] Intel Corporation, Intel. (2019). *Intel IoT Platform Reference Model and Products Solution Brief*. Accessed: Jan. 28, 2019. [Online]. Available: https://www.intel.la/content/www/xl/es/internet-of-things/iot-platform-solution-brief.html
[10] Microsoft. (2019). *Microsoft Azure—Subsystems and Cross-cutting*. Accessed: Jan. 28, 2019. [Online]. Available: https://azure.microsoft.com/en-us/solutions/architecture/subsystems-and-crosscutting/
[11] Amazon Web Services, Inc. or Its Affiliates. (2019). *AWS IoT Core*. Accessed: Jan. 28, 2019. [Online]. Available: https://aws.amazon.com/iot-core/
[12] Google. (2019). *Google Cloud IoT*. Accessed: Jan. 28, 2019. [Online]. Available: https://cloud.google.com/solutions/iot/
[13] L. Coetzee and J. Eksteen, "The Internet of Things—Promise for the future? An introduction," in *Proc. IST-Africa conf.*, Gaborone, Botswana, May 2011, pp. 1–9.
[14] B. Sterling, *Shaping Things*. Cambridge, MA, USA: MIT Press, 2005, p. 152.
[15] H. Kopetz, "Internet of Things," in *Real-Time Systems*, 1st ed. Boston, MA, USA: Springer, 2011, ch. 13, pp. 307–323, doi: 10.1007/978-1-4419-8237-7_13.
[16] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of Things: Vision, applications and research challenges," *Ad Hoc Netw.* vol. 10, no. 7, pp. 1497–1516, Sep. 2012, doi: 10.1016/j.adhoc.2012.02.016.
[17] T. S. López, D. C. Ranasinghe, M. Harrison, and D. McFarlane, "Adding sense to the Internet of Things: An architecture framework for smart object systems," *Pers. Ubiquitous Comput.* vol. 16, no. 3, pp. 291–308, Mar. 2012, doi: 10.1007/s00779-011-0399-8.
[18] S. Sharma, V. Chang, U. S. Tim, J. Wong, and S. Gadia, "Cloud and IoT-based emerging services systems," *Cluster Comput.*, vol. 22, pp. 71–91, 2018, doi: 10.1007/s10586-018-2821-8.
[19] E. Griffor, C. Greer, D. A. Wollman, and M. J. Burns, "Framework for cyber-physical systems: Volume 1, overview," NIST, Gaithersburg, MD, USA, Tech. Rep. 1500-201, Jun. 2017, p. 79, doi: 10.6028/NIST.SP.1500-201.
[20] H. Derhamy, J. Eliasson, J. Delsing, and P. Priller, "A survey of commercial frameworks for the Internet of Things," in *Proc. IEEE 20th Conf. Emerg. Technol. Factory Autom. (ETFA)*, Luxembourg, U.K., Sep. 2015, pp. 1–8.
[21] C. C. Aggarwal, N. Ashish, and A. Sheth, "The Internet of Things: A survey from the data-centric perspective," in *Managing and Mining Sensor Data*, C. Aggarwal, Ed. Boston, MA, USA: Springer, 2013, ch. 12, pp. 383–428, doi: 10.1007/978-1-4614-6309-2_12.
[22] M. Elkhodr, S. Shahrestani, and H. Cheung, "The Internet of Things: Vision & challenges," in *Proc. Tencon-Spring*, Sydney, NSW, Australia, Apr. 2013, pp. 218–222, doi: 10.1109/TENCONSpring.2013.6584443.
[23] D. L. Brock, "The electronic product code (EPC)," MIT Auto-ID Center, White Paper MIT-AUTOID-WH-002, 2001. Accessed: May 20, 2015. [Online]. Available: http://cocoa.ethz.ch/media/documents/2014/06/archive/MIT-AUTOID-WH-002.pdf
[24] K. Ashton, "That 'Internet of Things' thing," *RFiD J.*, vol. 50, pp. 97–114, Jun. 2009. [Online]. Available: https://www.rfidjournal.com/articles/view?4986
[25] S. Sarma, D. L. Brock, and K. Ashton, "The networked physical world," MIT Auto-ID Center, White Paper MIT-AUTOID-WH-001, 2001. Accessed: May 20, 2015. [Online]. Available: http://cocoa.ethz.ch/downloads/2014/06/None_MIT-AUTOID-WH-001.pdf
[26] L. Atzori, A. Iera, and G. Morabito, "Understanding the Internet of Things: Definition, potentials, and societal role of a fast evolving paradigm," *Ad Hoc Netw.*, vol. 56, pp. 122–140, Mar. 2017, doi: 10.1016/j.adhoc.2016.12.004.
[27] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the Internet of Things," in *Proc. 1st Ed. MCC Workshop Mobile Cloud Comput.*, 2012, pp. 13–16.
[28] C. da Silva, "Instrumentation of an engineering system," in *Sensors and Actuators: Engineering System Instrumentation*, 2nd ed. Boca Raton, FL, USA: CRC Press, 2015, ch. 1, pp. 1–34.
[29] A. Rayes and S. Salam, "The things in IoT: Sensors and actuators," in *Internet of Things From Hype to Reality*, 1st ed. Cham, Switzerland: Springer, 2017, ch. 3, pp. 57–77, doi: 10.1007/978-3-319-99516-8_3.
[30] L. Toka, B. Lajtha, E. Hosszu, B. Formanek, D. Gehberger, and J. Tapolcai, "A resource-aware and time-critical IoT framework," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Atlanta, GA, USA, May 2017, pp. 1–9.
[31] H. Zhou, A. Taal, S. Koulouzis, J. Wang, Y. Hu, G. Suciu, Jr., V. Poenaru, C. de Laat, and Z. Zhao, "Dynamic real-time infrastructure planning and deployment for disaster early warning systems," in *Computational Science—ICCS* , vol. 10861, Y. Shi, H. Fu, Y. Tian, V. V. Krzhizhanovskaya, M. H. Lees, J. Dongarra, and P. M. A. Sloot, Eds. Cham, Switzerland: Springer, 2018, pp. 644–654.
[32] C. Greer, M. Burns, D. Wollman, and E. Griffor, "Cyber-physical systems and Internet of Things," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. NIST SP 1900-202, Mar. 2019.
[33] L. Chen, S. Thombre, K. Jarvinen, E. S. Lohan, A. Alen-Savikko, H. Leppakoski, M. Z. H. Bhuiyan, S. Bu-Pasha, G. N. Ferrara, S. Honkala, J. Lindqvist, L. Ruotsalainen, P. Korpisaari, and H. Kuusniemi, "Robustness, security and privacy in location-based services for future IoT: A survey," *IEEE Access*, vol. 5, pp. 8956–8977, 2017, doi: 10.1109/access.2017.2695525.
[34] C. Xiaojun, L. Xianpeng, and X. Peng, "IOT-based air pollution monitoring and forecasting system," in *Proc. Int. Conf. Comput. Sci. (ICCCS)*, Noida, India, Jun. 2015, pp. 257–260, doi: 10.1109/iccacs.2015.7361361.
[35] K. Zheng, S. Zhao, Z. Yang, X. Xiong, and W. Xiang, "Design and implementation of LPWA-based air quality monitoring system," *IEEE Access*, vol. 4, pp. 3238–3245, 2016, doi: 10.1109/access.2016.2582153.
[36] Awair. (2018). *Know What's in the Air You Breathe—Awair*. Accessed: Dec. 13, 2018. [Online]. Available: https://getawair.com/

JORGE EDUARDO IBARRA-ESQUER (Member, IEEE) received the M.Sc. degree in computer science from the Center for Scientific Research and Higher Education at Ensenada (CICESE), in 2001, and the Ph.D. degree in computer science from Universidad Autónoma de Baja California (UABC), in 2019. Since 2002, he has been a Professor and a Researcher with the Facultad de Ingeniería, UABC, where he is currently in charge of student trajectory analysis. His research interests include the Internet of Things and data mining, and he has taken part in research projects related to improving the learning processes for students in the computer engineering major. He is a member of National Researcher of Excellence (SNI) and a member of the Mexican Academy of Computation (AMEXCOMP).

FÉLIX FERNANDO GONZÁLEZ-NAVARRO received the master's degree in systems engineering and the Ph.D. degree from Universitat Politècnica de Catalunya, Barcelona, Spain, in 2011. He is an Engineer in computer science with the Universidad Autónoma de Baja California (UABC), Mexicali, Mexico. He took advanced studies in artificial intelligence at the Universitat Politècnica de Catalunya. He is currently heading the Artificial Intelligence Laboratory, UABC. He is a Level 1 National Researcher of Excellence (SNI 1), a member of the Mexican Society of Artificial Intelligence (SMIA), and a member of the Mexican Academy of Computation (AMEXCOMP).

J. SALVADOR SÁNCHEZ (Senior Member, IEEE) received the B.Sc. degree in computer science from the Universidad Politécnica de Valencia, Spain, in 1990, and the Ph.D. degree in computer science engineering from Universitat Jaume I, Castelló de la Plana, Spain, in 1998. He is currently a Full Professor with the Department of Computer Languages and Systems, Universitat Jaume I, and the Head of the Pattern Analysis and Learning Laboratory. He is author or coauthor of more than 200 scientific publications, co-editor of three books, and a Guest Editor of several special issues in international journals. His research interests focus in the fields of pattern recognition, machine learning, and data mining, including classification, feature and prototype selection, ensembles of classifiers, data analysis, and reinforcement learning. He serves as an Associate Editor for *Pattern Analysis and Applications* journal and for the Progress in *Artificial Intelligence* journal. He is currently the President of AERFAI (the Spanish Association for Pattern Recognition and Image Analysis).

BRENDA LETICIA FLORES-RÍOS received the master's degree in computer science from the Center for Scientific Research and Higher Education of Ensenada (CICESE) and the Ph.D. degree in sciences from the Universidad Autónoma de Baja California (UABC). She is an Engineer in computational systems from the Technological Institute of La Paz. She is currently heading the Software Engineering Laboratory, Department of Computing and Information Technology, Institute of Engineering, UABC, Mexicali campus. She is a Level 1 National Researcher of Excellence (SNI 1) and a member of the Mexican Academy of Computation (AMEXCOMP).

MARÍA ANGÉLICA ASTORGA-VARGAS received the M.Sc.Eng. degree. She is currently pursuing the Ph.D. degree in computer science. She is currently a Professor with the Computer Systems program, Universidad Autónoma de Baja California (UABC). Her research interests include software engineering, software process improvement, and the impact of knowledge management on software engineering. She has participated as a Consultant in the implementation of software process improvement initiatives and an Appraisal Team Member in CMMI-DEV SCAMPI A levels 2 and 3.

MARIA LUISA GONZÁLEZ-RAMÍREZ received the master's degree in electronics engineering with a major in telecommunications, in 2009. She is currently pursuing the Ph.D. degree in computer science with UABC. She is a Computer Engineer with Universidad Autónoma de Baja California (UABC). She has also been working as a Professor and a Researcher in the computer engineering major with UABC, since 2000. Her research interest focuses in the field of the use of information technologies in engineering education.