# Internet of Everything (IoE) Taxonomies

Subjects: Automation & Control Systems
Contributor: Viviane Cunha Farias da Costa

The paradigm of the Internet of everything (IoE) is advancing toward enriching people's lives by adding value to the Internet of things (IoT), with connections among people, processes, data, and things. This paper provides a survey of the literature on IoE research, highlighting concerns in terms of intelligence services and knowledge creation. The significant contributions of this study are as follows: (1) a systematic literature review of IoE taxonomies (including IoT); (2) development of a taxonomy to guide the identification of critical knowledge in IoE applications, an in-depth classification of IoE enablers (sensors and actuators); (3) validation of the defined taxonomy with 50 IoE applications; and (4) identification of issues and challenges in existing IoE applications (using the defined taxonomy) with regard to insights about knowledge processes.

Keywords: Internet of everything ; Internet of things ; IoE ; IoT ; taxonomy ; sensors ; big-data ; knowledge

## 1. Introduction

The Internet of everything (IoE) is a term that was first defined by CISCO in 2012 [1] as a network of networks that reunites people, processes, data, and things in network connections more significant and valuable than ever [2][3][4]. While the Internet of things (IoT) is a dynamic global network infrastructure [5] concerned about things (i.e., physical devices, accessed through the Internet), IoE lays an upper foundation over IoT and is concerned with intelligent network connections and technologies [6][7][8][9].

IoE supports creating new capacities, better-off competencies, and outstanding economic opportunities for businesses and society [1]. For Fiaidhi and Mohammed [10], IoE expands on the IoT concept by connecting devices and people in one network. Beyond the concept of IoT, the IoE paradigm covers a wide range of Internet-based concepts; for example, the Internet of people (IoP), which considers social networks and connections among people; and the industrial Internet (II), which is focused on data of interest to industry [7]. The concept of IoE incorporates nanosensors in diverse objects using nano-networks. It provides access to data that had previously been impossible to sense. This technology transition involving IoE is a concept called the Internet of Nano things [11].

With more relevant connections than machine-to-machine communications, IoE has enabled the global democratization of skills, including person-to-machine and person-to-person connections [12][13].

Accordingly, Auger et al. [4] argue that IoE extends the concept of IoT by exceeding the connections of things and integrating common impacts, risks, and economic benefits for the novel interconnected society. Thus, "intelligent services", together with the "things", represent the "everything" in IoE [14].

For Raj and Prakash [13], IoE is a superset of IoT and requires advanced capabilities within the area of information sharing. The IoE paradigm can extract and analyze real-time data collected from diverse and heterogeneous IoE environments, from simple sensors and actuators to complex robotic devices, and from autonomous service agents to human actors [3]. Thus, IoE applications require appropriate measures to be taken in the initial phases of their design and implementation [13]. Artificial intelligence (AI) integrated into smart devices provides the increasing deployment of innovative and useful IoE-based applications, where people and things interact appropriately within a social context and multi-user environment [11].

Processes are the core of IoE; they represent network "connections" and real-time data/information flows [15] among IoE nodes [16]. The result is smartness and intelligence [17], and real-time insights working in concert [18], far beyond IoT context disruptions [19], addressing the societal and organizational needs for more data and more actionable intelligence.

Actions and interactions within the IoE environment create and expand knowledge in a transcending process through which entities (people, things, and data) acquire new knowledge and new interactions are created in knowledge-creation cycles [20]. This transformation from data to knowledge in IoE provides essential insights and various possible applications

[21][22].

Value-generating activities come through knowledge processes that filter data, information, and knowledge into a decision context, in which it becomes actionable intelligence [23]. A knowledge-based strategy for selecting and managing technologies and decision support artifacts (big data, data, information, knowledge, and intelligence) assists in the management and governance of data and technologies to ensure great benefit from IoE's capacity to provide enhanced intelligent services.

Figure 1 shows the "four enablers" (people, data, processes, and things) in IoE.

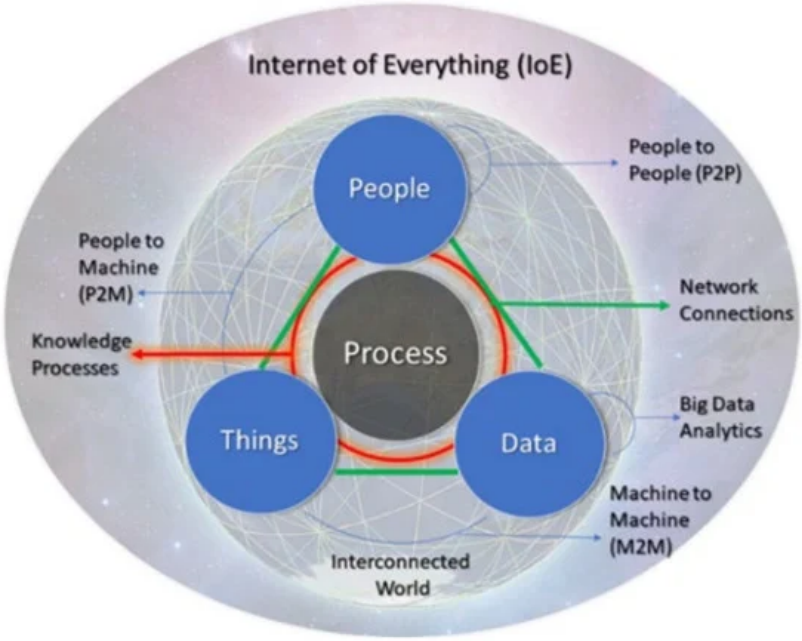


**Figure 1.** Internet of everything, adapted from [16].

Several taxonomies for IoT [24][25][26][27][28][29][30] and IoE [6][13][15][17][31][32], have been proposed. However, there are challenges concerning the ranking and managing of knowledge processes in IoE applications.

First, there is still a fragmented framework: (1) A lack of consensus and new demands are unique to the IoE context (e.g., empowering people and providing intelligence services and insights through the collaboration of IoE enablers [sensors and actuators]); and (2) A lack of consideration for the integration of IoE connections (machine-to-machine, people-to-people, and people to machine) from perspectives that support the high heterogeneity of existing IoE devices and the expected value creation in IoE applications—the perspective of knowledge that refers to actions, comprehension, and meaning derived from the information inside a context; the perspective of sensors and actuators physical characteristics and usage in IoE context, the perspective of information observation within ever-changing IoE contexts, and the perspective of infrastructure capabilities and resources required.

The successful adoption of a particular technology depends on the comprehension of its use and features [33]. Research on knowledge management has focused on understanding the complex relationships between data, information, and knowledge creation, and how they are impacted and benefited by the sources (or spaces) of data and information and the contexts in which they are analyzed and shared [34]. Therefore, an in-depth classification of IoE enablers (sensors and actuators) identifies issues and challenges in existing IoE applications regarding insights about managing knowledge processes that create value from the IoT context.

## 2. Proposed IoE Taxonomy

This section presents the proposed IoE taxonomy. For the conception of this taxonomy, we selected a method proposed by Nickerson et al. [35] for taxonomy development that has been adequately addressed for taxonomy development in the information systems (IS) domain. The proposed taxonomy identifies and categorizes sensors, attributes, and characteristics that are essential for developing IoE applications. This study is the first attempt to represent the types of knowledge (from sensors and actuators) in the IoE domain and how knowledge processes lead to intelligent services in IoE applications.

The development of an IoE taxonomy involves determining the characteristics of the sensors in IoE applications that arise from a refinement process at various stages to sufficiently satisfy the following qualitative attributes from Nickerson et al. [35] regarding the taxonomy:

- Concise: has a limited number of dimensions and characteristics, restricted to what is relevant and understandable;
- Robust: contains suitable dimensions and characteristics to distinguish the objects of interest;
- Comprehensive: includes appropriate and enough dimensions to classify all known objects within the domain under regard;
- Extendable: allows for the insertion of additional dimensions and characteristics within a size to contemplate new incorporated objects;
- Explanatory: provides useful explanations and valuable descriptions of the nature of the objects under study.

Additionally, developing a useful taxonomy is a search process of design [35]. Kotis et al. [36] presented requirements for a well-defined collaborative and iterative methodology, addressing practical aspects that drive consensus on developments —a “live” method of development in which the artifacts evolve over time. An artifact must preserve its liveness, evolution, and reusability during its life cycle (i.e., it may be in-use in a particular time or instant, be under constant maintenance or update and be used in applications/projects beyond its original purpose).

We followed an iterative method during the development process, as suggested by Nickerson et al. [35], and a conceptual to the empirical approach, based on the surveyed existing taxonomies related to IoT and IoE (Section 3). Furthermore, a collaborative approach that relied on authors´ insight, experience, intuition led to proper identification of the proposed dimensions and characteristics, as resumed in the following stages of the development.

For Nickerson et al. [35], the taxonomy’s purpose (meta-characteristic) drives the taxonomy’s dimensions and characteristics. Each element or classification proposed in the taxonomy should be a logical outcome of the meta-characteristic. Our aim was “to guide the identification of critical knowledge in IoE applications, an in-depth classification of IoE enablers (sensors and actuators) based on the knowledge they provide in intelligent tasks”.

The development process ended when both objective and subjective conditions have been met [35]. During the iterations processes, new characteristics were identified and included, and when any characteristic turned out not to be relevant, they were eliminated after consensus. Further analysis succeeded until reach the ending conditions, engaging authors in close collaboration towards shaping commonly agreed dimensions and characteristics. We used two objectives ending conditions: no new dimensions were added in the last iteration, and every characteristic was unique within its dimension. Subjectively, the process ended when the taxonomy was determined to be concise, robust, comprehensive, extendible, and explanatory [35] and fulfilled the quality requirements of liveness, evolution, and reusability [36] that are suitable to dynamics of the IoE pervasive environment.

Accordingly, ranking knowledge in IoE sensors is a matter of eliciting the main characteristics in IoE applications. In order to understand the IoE domain, we applied specific questions by answering the 4 ws (what, when, who, and where) and 1 h (how) identified using the 4W1H methodology [37][38]. This methodology addresses the challenge imposed due to the high heterogeneity of existing IoE devices. A similar approach was proposed in [39] to measure the quality and value of information when considering the value created by the IoE in applications. These questions guided the definition of the following four complementary categories that drive the purpose of taxonomy dimensions and characteristics:

- (a) Knowledge: regarding knowledge in action; that is, the artifact or information inside a context (*what*) with comprehension and meaning;
- (b) Type: typifies sensors and actuators—*who* they are, their physical characteristics, their usage, and their role in IoE context: sensors or actuators in cyber, physical, or cyber-physical presentation;
- (c) Observation: the physical context in time (*when*) and space (*where*); that is, the instant and location that the information content was sensed or perceived within ever-changing IoE contexts;
- (d) Capabilities: *how* the information is flowing, the infrastructure capabilities, and the resources required.

For this stage of development, we used the top-down development process, starting with defining the most general categories (*knowledge, type, observation,* and *capabilities*). We then selected dimensions and characteristics previously derived from a theoretical foundation from reviewing the related literature, and grouped them in related *knowledge, type,*

*observation,* and *capabilities* categories, revealing the resulting taxonomy. Our IoE taxonomy consists of four categories (see Figure 2) and groups 18 dimensions, each comprising of mutually exclusive and generally collectively exhaustive characteristics.

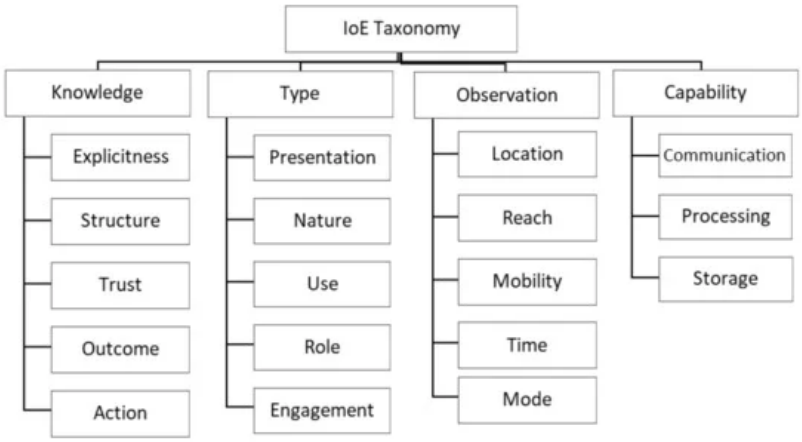


**Figure 2.** IoE taxonomy.

## 2.1. Knowledge

The *knowledge* category contains five dimensions related to knowledge creation and information flow: explicitness, structure, trust, outcome, and action. Each has its own specific sub-dimensions or characteristics, as shown in Figure 3.

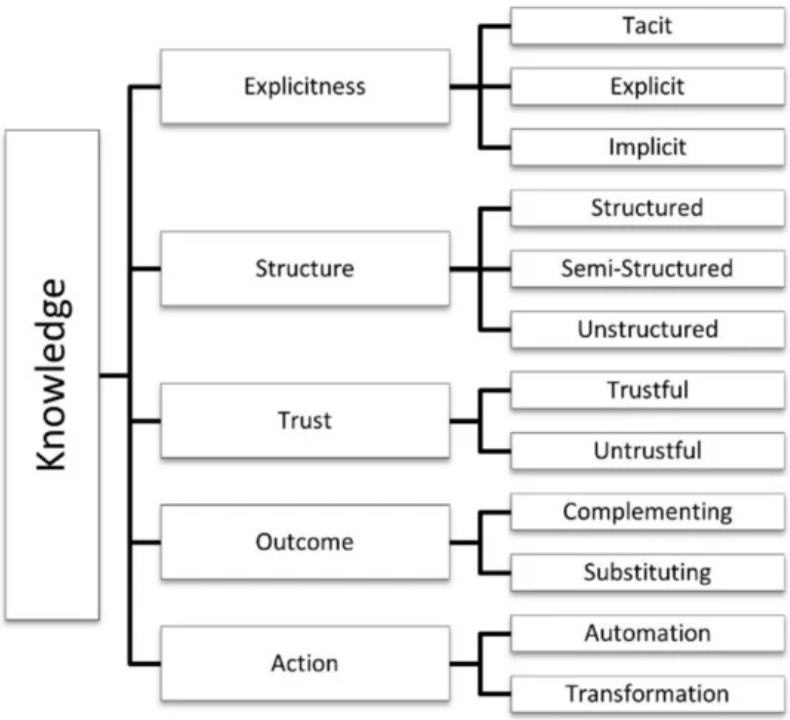


**Figure 3.** IoE Taxonomy: knowledge category with dimensions and characteristics.

### 2.1.1. Explicitness

IoE environment architectures consist of IoT standard architecture [40], but with the addition of the human element (which acts as a node) and intelligent services to the IoT network [32]. knowledge discovery approaches used in developing IoT solutions [41], which involve sharing information from smart objects, should be optimized by examining how humans process data sources of information to form knowledge [42]. For Perera et al. [43], this requires knowledge from different perspectives, for example, knowledge of sensors, applications, users, and so forth. Moreover, these uncovered knowledge patterns are analyzed and integrated for subsequent use in real time, using multiple knowledge management approaches [44][45][46]. The intelligence of connected things varies from non-existent to absolutely rational [24]. There are different kinds of knowledge, and it demands distinct representations. A taxonomy is a central link between knowledge engineering and knowledge management [47]. Regarding explicitness, this work classifies knowledge provided by sensors in IoE applications into three distinct types:

- Tacit: This knowledge is rooted in actions, experiences, and involvement in specific contexts. Tacit knowledge consists of people's knowledge based on intuitive evaluations of sensory inputs and perceptions, which is sometimes hard to express (i.e., feelings, beliefs, insights, values, and ideals) [48]. The increase of human senses through sensor and data fusion and context awareness is the essence that supports smarter wearable devices for relating mutually with human cognitive memories [49].

- Explicit: This knowledge is codified and articulated knowledge (i.e., the form of knowledge that is easy to codify using formal language, procedures or principles) [48]. Explicit knowledge from hard sensing-based data acquisition results in discovering hidden patterns in the aggregated sensor data [50][51]. The explicitness denotes awareness of a fact or artifact, which means the application of knowledge [49] from efficient scheduling of the resources in IoE applications [41] [52]. Sensors continuously generate enormous amounts of data, with the value created being conditioned to its analysis.

- Implicit: Knowledge is not explicitly represented in the knowledge base but is inferred from it by using several assumptions [53]. Thus, implicit knowledge may be implicit information intertwined in information systems and data sources [48]. Myriad data analytic algorithms can be executed to extract a higher level of information from sensed data [52]. The value created by implicit knowledge emerges from machine learning and AI technologies, mainly in machine intelligence services [54]. It consists of outputs to make predictions oriented toward decision support and automation in diverse IoE application scenarios [55].

#### 2.1.2. Structure

The combination of data streams with background knowledge enables meaningful analysis to derive higher levels of abstraction and deliver quality actionable information to IoE services [56][46][52]. Sensor data are a piece of explicit knowledge with metadata characterizing the body of evidence [39]. The distinctions between data, information, and knowledge are largely irrelevant [48]. Knowledge is created by transforming the multiple data formats collected (structured, semi-structured, and unstructured) [57] into high-level information [43][58][45][59], and useful knowledge patterns [43]. Descriptions of these data formats are given below:

- Structured: These data have an identified format and a relational structure, frequently accessed using a standard SQL-type language and stored in relational database management systems. Typical examples of structured data are string, numeral, and date. [60].

- Semi-structured: These data cannot be managed by conventional database management system techniques, but the interpretation and analysis of these data require comprehensive and intelligent rules. Typical examples of semi-structured data are extensible markup language (XML) and JavaScript object notation (JSON) data. [61][54][60].

- Unstructured: These data do not follow any specific format and are often represented in a rather complex structure that contains hidden relationships. Examples of unstructured data are videos, text, time information, and geographic location [62]. With the amount of data generated by sensors, devices constantly produce large volumes of structured, unstructured, and semi-structured data, which results in "big data" [63][64].

IoT processing of sensing data streams provides ubiquitous sensing services [50][55][65]. Data aggregation processes are vital for improving the quality of the designed system [66]. Big data technologies assist in data processing [44], the uncovering of new and valuable insights and information from incorporated data sources [28][67], and in improving prediction and decision-making [55].

#### 2.1.3. Trust

In a hybrid human-based and device-based environment, such as IoE, data's trustworthiness can be estimated mostly by the sensor nodes' reputation [68]. Trust management is a decisive challenge for data access and data storage on IoE applications [69][70].

Dynamic and heterogeneous network environments and the diversity of devices connected in the IoT generate an extensive array of potential security threats [27][71][72][73]. The network interoperability level should address concerns such as the security of the data to be transmitted [58], and a coherent IoT architecture would provide a layer of data security [74] [75] since the IoT has no uniform architecture. Approaches and methods to improve users' awareness about the effects of potential IoT threats may mitigate the risk of exposure [76][77][39][78].

Knowledge assets vary in veracity levels [48], between the extremes of truth and untruth [79]. In some broad sense, the value of knowledge depends on the quality of the sensors' information. Security approaches must be made self-sufficient and autonomic, with the minimal manual human intervention [76]. Sensor networks' applications need support regarding privacy, security accuracy, timeliness, relevance, completeness, and provenance [80][39]. The data source's reputation

represents the source's truthfulness in providing quality content to handle changing external requirements and contexts [54]. Any direct or indirect connections of user information with connected objects within IoT landscapes categorize trust in communication and security issues [70][74]. The trust values are considered based on the reliability of devices and the level of security and trust engaged in implementing and operating the connectivity [81][82]. Knowledge of sensors and sensor data in IoE applications is either trustful or untrustful:

- Trustful: Based on protecting both user and service provider privacy precedents [62]. Constituting meaningful identity, using trusted communication paths, and preserving contextual information is essential to guarantee the protection of users' privacy in the IoE environment [83]. The work in [84] addressed the security of IoT objects and privacy issues by merging identification, authentication, and authorization into one argument: access control. The security dimension encompasses five concepts: access control, confidentiality, integrity, availability, and non-repudiation. Different studies have covered concerns such as anonymity, liability, and moral, ethical, legal, cultural, and regional parameters, among other things [85][86][87][88].
- Untrustful: False or misleading data culminates in wrong decisions and critical consequences and lead to uncertainty at all knowledge transformation levels. Incompleteness in data occurs at the lower layer of the sensor readings or raw data collected. Vagueness frequently appears at a higher level of contextual information [68][67]. Possible security risks associated with IoT data are the heterogeneity of the smart devices and the nature of sensed data or authentication among different trust domains [89], which further complicates access control decisions.

#### 2.1.4. Outcome

The IoE paradigm impacts human interaction with everyday objects. Considering the type of information exchanged between humans and the system [90], the expected outcomes from IoE applications provide multiple tiers of cognition with the fine-tuning sensory acquisition from heterogeneous contexts [91]. Distinct levels of collaboration between IoE resources require efficient solutions. Human sensors peculiarities contemplated by collaboration theory and technical aspects of user interaction are challenges in computer network theory [28]. It is imperative to provide awareness of collective intelligence and where the intelligence is [81], representing the outcomes expected in designing the IoE solutions, based on the application domain [28][59].

The outcome dimension refers to the degree to which knowledge sources (things and humans) contribute to knowledge creation in IoE intelligent services. Relevant knowledge contributions from human or non-human enablers (sensors or actuators) either complement or substitute (or both in some cases) to provide improved outcomes reached through knowledge sharing processes, and sometimes automating or transforming traditional tasks [84] into IoE environment disruptions:

- Complementing: Represents knowledge sharing between IoE sensors and actuators. Complementing outcomes occurs when humans utilize mobile devices like sensors to collect their observations and information about the environment and infrastructures [25][92][77] or when artificial intelligence complements human knowledge.
- Substituting: Provides insights and novel interpretation of reality to enhance the quality of life (livability), regarding knowledge acquisition as the "core element" and the realization of "intelligence" [93].

#### 2.1.5. Action

The Action dimension refers to knowledge creation. Actionable intelligence is meaningful for humans to promote automated processes [92], ranging from creating value when used in a specific usage context [25][39][94] to transforming and changing the state of their environment [24]. Big data analytics aims to improve the understanding of data, thereby supporting useful and timely decision-making with the refined information gathered [62][50][67].

The goals of IoT systems range between general and specific and include monitoring, reducing costs, and improving processes [73].

For Russell et al. [94], even in the case of uncertainty, a rational agent is one that acts to achieve the best outcome or the best-expected outcome. There is a close interrelationship between intelligence and automation [84], or creating and pursuing goals through transformation. Sensor information in IoE applications provides either automation or transformation of the IoE environment, which are defined as follows:

- Automation: the aptitude to make cognitive decisions related to a given situation, which guarantees the right action is performed. The automation of tasks and dependency on machines may reduce human abilities [60]. When combined with AI and machine learning, new applications will benefit from automated decision-making [65], with efficient usage of

network resources, minimization of operational costs, coordination of computational resources, and efficient and effective data management mechanisms [71] associated with the quality of experience [59][95].

- Transformation: an enormous number of raw observations (created by the machine and human sensors) can be transformed into higher-level abstractions [91] that are meaningful for human or automated decision-making processes [84]. When an IoE solution provides transformation, smart things act independently, with minimal or no human intervention [92]. With the support of wireless communications and AI, humans benefit from improvements in technological advancements [50][54] by collecting, modeling, and reasoning the context [43].

Considering how actions generate changes in the environment to achieve the desired goal, automation and transformation processes may occur in the short or long term or may represent a prominent solution. Some works have explored the implications of the IoE for value creation and decision-making provided by smart things and big data [15][85]. However, our study is concerned with how humans respond and interact with the environment in assisting the evolutions of future systems (defined in [15]), which can be:

- Reactive: having the ability to promptly react to a changing environment;
- Adaptive: having the steadier ability to adapt their behavior to changes;
- Predictive: having the ability to use computation and analytics techniques to identify relevant patterns, in-depth knowledge of the environment, and the most appropriate solutions or possible evolutions to each IoE system situation.

## 2.2. Type

The *type* category contains five dimensions or subcategories for the classification of sensors and actuators: presentation, nature, use, role, and engagement. Figure 4 highlights the type category, its dimensions, and characteristics.

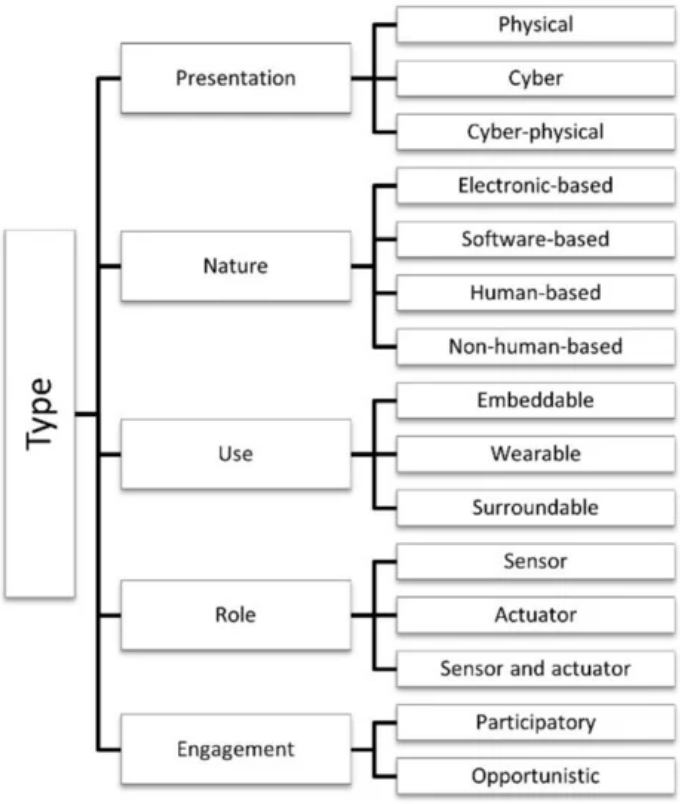


**Figure 4.** IoE Taxonomy: type category, its dimensions, and characteristics.

### 2.2.1. Presentation

Presentation refers to the physical aspects of sensors and actuators that interact with the physical world. The physical and virtual world can be merged by integrating computation and physical processes in one of the following ways: a) physical, b) cyber or virtual, and c) cyber-physical or logical [30][80][96][97][98][90].

Humans are content receivers and can act as a sensor collecting data for the sensory systems or actuators performing actions, but humans are also content providers who share diverse and relevant types of spatial-temporal data [99][100][77]. The physical dimension characterizes the mobility of the system's things and the dependency of the collaboration of human and non-human devices [28][85]. Accordingly, sensors and actuators can be classified as follows:

- Physical: Physical entities are tangible devices that generate sensor data or perform actions changing the environment. The data retrieved from physical sensors represent a low-level context [43]. Examples of physical sensors are temperature sensors, pressure sensors, biosensors, light sensors [6], and human sensors [101]. Examples of the physical actuator are a door opener actuator invoked by an intelligent system and human actuators.

- Cyber or virtual: An abstract information entity that invokes sensor or actuator functions but does not directly interact with the physical world. Examples of cyber or virtual entities are computer programs and systems, communication processes, and monitoring activities with no physical body (e.g., sensing web service) [92][51][64]. Virtual entities use web services technology to send and receive data from many sources [43].

- Cyber-physical or logical: Represents the connection of the cyber and physical worlds as a combination of physical and virtual entities to generate meaningful information [25][102]. Similar to virtual entities, they commonly use web services technology to send and receive data and interact with the physical world [43]. They are autonomous objects augmented with sensing, actuating, processing, storing capabilities [86]. Examples of cyber-physical entities are web services dedicated to providing weather information resulted from physical sensors that sense weather information and virtual sensors that process historic weather data.

#### 2.2.2. Nature

This dimension is related to sensor or actuator knowledge, intertwined with its architecture and functionality [103]. A sensor is anything that observes, and an actuator is anything that performs defined actions [104]. People can be modeled as sensors and actuators [94], so anything that acts individually to perform a task in the IoE context is an individual IoE device [99]. Knowing the nature of knowledge source devices is crucial for publication, discovery, sharing, reuse, and integration of information within the IoE environment [105]. Human beings with dedicated roles, as well as machines, devices, and services [101][65][74], implies system constraints when it interacts with the physical space [80]. Humans are content receivers through the sensory systems and also content providers—mainly through sensing and actuating abilities [100][106], and through tacit knowledge and experiences that can affect their actuations in IoE applications and cognitive tasks.

The level of autonomy of an IoE sensor or actuator (human or non-human) refers to its ability to act independently [24][102] [81]. Several works have identified entities—sensors/actuators—types according to activities carried out in physical and virtual worlds [30][68][96].

According to their built-in nature, sensors and actuators in IoE are classified [96] as follows:

- Electronic-based: Define physical IoT devices constituted of electronic or mechanical systems that sense or actuate physical phenomena.

- Software-based: Define virtual entities that process information from data sources or generate analytical results.

- Human-based: Refers to humans or virtual entities based on knowledge provided or expressed by human perception about any phenomena arising in their physical, virtual, or social environment.

- Non-human-based: Define biotic sensors/actuators or virtual entities based on knowledge data provided by biotic perception about any phenomena arising in their physical environment. In the constantly growing area of animal cognition, sensor networks monitor the health and well-being of animals in livestock herds and in animal surveillance applications [107].

#### 2.2.3. Use

Refers to the physical characteristics of physical IoE sensors or actuators related to their usage in a particular application. The devices inherit the attributes of their owners or of the entities or places [98] to which or where they are attached [103][51] [81]. A wide variety of objects—a group of infrastructures and devices [108] such as embedded devices, sensors, and actuators—have integrated communication and strong interactions to create a ubiquitous environment [56][65][74]. A taxonomy for IoT sensors communicates how distinct types of sensors are combined and used in specific application domains [105].

Smutný [29] described things according to how they are used or applied in relation to humans:

- Embeddable: Things that are in the user or under the user's skin, that are non-autonomous, or embedded in carry-on devices [50]. The level of autonomy ranges from human-companion device tasks [77] to opportunistic devices, which decide and act independently [24][28]. For example, a mobile phone is a ubiquitous, convenient and user-friendly device and has many sensors embedded [109], which is why it has turned into a global mobile sensing device [97].

- Wearable: Things that rest on a person's body or can be used, worn, or attached to their owners and enable accurate detection of the wearers' motions [61][100][58][110].

- Surroundable: Things that are autonomous, near or around the user, but which have no physical contact with the user. Recently, several non-contact techniques have been interpreted as highly valuable in dealing with highly infectious diseases such as COVID-19. In a pandemic scenario, non-contact sensing was able to detect information without direct contact with the patients and without devices physically touching the body [111].

#### 2.2.4. Role

IoT devices have sensing and actuating capability according to defined rules under various scenarios [99][105]. They perform sensing and actuating functions [24][26][92] that help in interacting with the physical environment [109]. An IoE device or enabler can be a sensor, an actuator, or a sensor and actuator [108][93][65].

- Sensor: A device that observes and senses. Sensing is a read operation over a context entity. The data collected by a sensor is stored and processed intelligently to derive useful inferences and to support the decision-making process [80]. Sensors are monitor devices and physical entities, which provide the information required to immediately control actuators, whereas actuators act on the physical entity or control other things [28][101][82].

- Actuator: Affects a particular domain of the physical space or a combination of both. Actuation is a write operation over a context entity, in which the conceptual entity represents the domain of a sensor or an actuator [108]. Actuators perform the decided actions and effect a change in the environment [43][85][109].

- Sensor and actuator: This device is a hybrid of the two previous categories, and it can gather data and act within its environment.

Processing and analytics (fixed process or algorithm, machine learning, or AI) do not fit within this classification [81].

#### 2.2.5. Engagement

Participation is an interaction between people with existing technologies and occurs at different engagement levels [97]. Engagement refers to sensing tasks. In data acquisition, it can be both opportunistic and participatory, and it provides sensory information that collectively forms knowledge.

For example, enhancing human senses is possible when machines interact with humans or provide remote operation in perceived real time in ubiquitous computing [91][100]. Cooperative smart things can interact with other entities of the IoE in order to achieve a unified objective [15]. With mobile crowdsourcing, the primary information shared voluntarily is user knowledge and opinion, along with location as the only sensor information [77]. The engagement of a sensor node in an IoE application is one of the following:

- Participatory: The IoE enabler (sensor node or actuator) is actively involved and actively reports observations [106]. It can provide information about the environment or surroundings, as well as any other sensory information that could be on social groups (social sensing) or with everyone (public sensing) or at the community level [68][97][65].

- Opportunistic: The IoE node has minimal or no involvement—it senses and monitors tasks running in the background. Embedding sensors trigger the data automatically (either periodically or based on events).

### 2.3. Observation

The *observation* category contains five dimensions or subcategories related to sensed context: location, reach, mobility, time, and mode. Figure 5 emphasizes the dimensions and their sub-dimensions or characteristics.

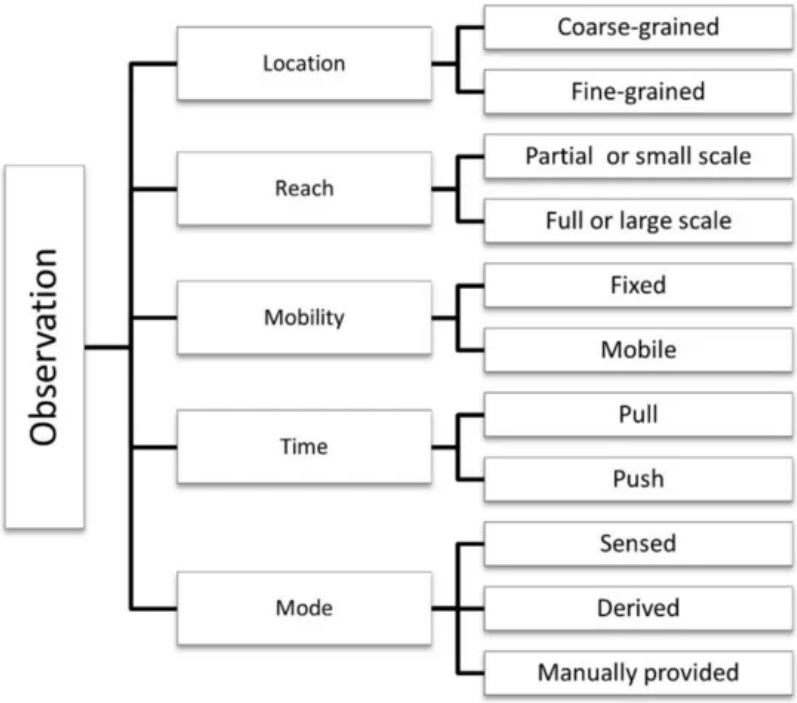


**Figure 5.** IoE taxonomy: observation category, its dimensions, and characteristics.

#### 2.3.1. Location

Location is used to describe the spatial context (physical context) of users/devices within a local or global network [24][81]. It represents the geophysical position of a sensor or actuator in absolute values, identifying the coordinates (latitude and longitude) or relative specifications through location tags [86], which is obtained manually or automatically [106][112]. It represents the definition of an area covered by a particular object [98]. Sensors that are randomly deployed get the required information about the target environment [113].

Location systems can be categorized as context-aware systems [110]. The precise location of an object is critical since location plays a critical role in context-aware computing [43][51][114]. Moreover, aggregation of knowledge patterns facilitates reduced data transfer in distant environments and minimizes bandwidth use [45]. Some physical measurement-based localization schemes are classified as coarse-grained and fine-grained [114].

#### 2.3.2. Reach

Reach classification distinguishes between individual and collective knowledge. It refers to an environment of sensing interest [56]. Sensors are becoming more sophisticated in technology advances, cheaper in price, and smaller in size. This evolution stimulates large-scale deployments [43], and dense geographical distribution [71].

The domain of interest represents the applicative domain in which the device is operative [98][113] and ensures that IoT services are accessible or reached only by authorized access [81][115].

The prevalence of mobile devices, such as smartphones, has triggered challenges for mobile networks worldwide [116], as well as novel classifications, such as collective knowledge classified into individual or group, internal or external, full or partial domains. For example, a conglomeration of sensor data stored on cloud infrastructure can be designed as big data sensing, and based on the reach of its sensing requests and requirements [64], it can be referred to as a) private, b) public, c) community, or d) hybrid big data sensing.

In crowdsourcing, regarding the boundaries of the individual scope in which crowds collaborators are immersed, the reach can be classified as ranging from small to large-scale (from a person to a group, community, city, and so forth) [28][77].

#### 2.3.3. Mobility

Mobility, which is also called monitoring continuity [43], is one of the main characteristics that enables identification of the state of sensors and actuators and their capability of movement [26][43][85][103][108][114], with significant implications on device operation, connectivity, and location management [30][109][114]. Devices are classified into two categories: static/immobile/fixed and mobile [26][93][41][81].

- Fixed/static/immobile: Objects that remain static to a specific location or cannot move. Their observations are restricted to a specific location, in a static or very constrained (in terms of mobility) environment that is not designed to move (relative to their point of installation) without being uninstalled.

- Mobile: The objects move [108], and their location may be calculated in absolute coordinates or relative to reference nodes in the network [113], requiring wireless communications to transmit data and allow configuration and control [81]. Their movement and mobility capability are controlled independently (or autonomously) or dependently through device users [103].

A self-moving device moves autonomously and relative to its setup/installation point, without being uninstalled (e.g., smart car), whereas a non-self-moving device does not move autonomously but can still move relative to its original location without being uninstalled [26][93].

Mobility of the things in the system is dependent on the collaboration of the items physically coupled with the humans in the system [28], as in crowdsensing applications, in which geographically dispersed users actively (participatory) or passively (opportunistic) collect data with their smartphones [92][110]. Classifications between mobility-agnostic and mobility-aware [41] highlight an approach that ignores knowledge about mobility and the ones that consider and exploit it for optimization [10].

Challenges related to mobility include frequent disconnections and handoffs, which affect perfect connectivity [117]. Mobility techniques in the cloud, fog, and edge architectures [71] support mobility, and other protocols apply routing and resource discovery mechanisms [85].

#### 2.3.4. Time

Time represents the instant of observation (i.e., timestamp) [98]. Information about time and location are critical features of some applications (called spatial-temporal-aware applications) that require tasks to make observations at a specific location during a defined period [106]. In [24], latency relates to the time an IoE system needs to answer to a stimulus. Interaction between IoE smart devices can influence the service's response time to end-users. The time interval between the initiation and the conclusion of the task is the response time [69][66][73].

The time dimension depends on how sensors are requested or provide data to the system in specific periods or on an ad-hoc basis (as software system makes a request), which is characterized as the following two distinct methods that were proposed in [66]:

- Pull method: The software component in the control of obtaining sensor data from sensors makes a requisition periodically (after specific intervals) or instantly obtains sensed data [66].

- Push method: The physical or virtual sensor pushes data to the software component in the control of obtaining sensor data periodically [43][66]. In many cases, a sensor observation can be the result of a local sensor data fusion [39].

Real-time applications monitor the state of the environment and react to changes accordingly and in a timely manner.

The deployment of IoE applications in real-world scenarios creates a massive amount of data from real-time interactions, usually at high data rates. It faces challenges as temporal data consistency related to the coherency between the value of the data in the system and its environment state [66]; and high latency during interactions [85], when inferred contexts evolve with time [37][45], and the exchanged data may not be accurate.

Hard real-time data cannot accept any delay; in contrast, soft real-time data can accept various bounded delays. Delay-tolerant applications can be categorized as nonreal time [71][66]. In offline circumstances, the delayed transmission may be crucial to address quality and security constraints [68][77].

In real-time situations, timeliness [67][66] describes data processing in a specific deadline, which is real time, near real time, or batch processing [81].

- Real time: refers to the immediate data processing to provide instant results for a time-sensitive application.

- Near real time: refers to situations when the delay time is still relevant for the application, but the computation process is not as immediate as real time.

- Batch-processing: refers to situations when data are first collected and processed at a predetermined interval or when a specified volume of data is available [68].

#### 2.3.5. Mode

The combination of sensors serving different purposes and data generated in IoE applications implies the need to classify data sources and information in the IoT context [105]. During real-time data harvesting, it can be challenging to determine the possible relationships among heterogeneous knowledge sources [67]. Smart device sensors are either active or passive sensors, depending on their usage and functionalities. If the sensor data collected are reflected in the same way as designed, this is called active functionality. However, sensors operate passively when collected data are interpreted or processed in new ways [17][77].

Eris et al. [28] defined how much interaction is required within the network in three levels of collaboration interdependence [28]:

- Pooled interdependence: The lowest level of collaboration, in which each collaborator barely contributes to the collaboration environment and benefits from the contributions of others. The collaborators neither synchronize nor negotiate the nature of each other's contributions.
- Sequential interdependence: The middle level, in which the contributions of one collaborator become the inputs to another collaborator contributions. In this case, there is a temporal ordering of the collaboration efforts.
- Reciprocal interdependence: The highest interdependence level, in which one collaborator's contributions are the next collaborator's inputs, and collaborators must also negotiate the nature of each other's contributions to the collaboration environment.

The Mode dimension refers to the way of linking the physical and digital world in order to acquire context [118], and it can be either sensed, derived, or manually provided:

- Sensed: Data gathered through sensors.
- Derived: Includes the sensed data stored in databases or the information generated by performing computational operations on sensor data. Data aggregation is the ground for the application's workflow and unconditionally impacts the application's quality. Distinct aggregations may have specific requirements to be supported by design [66].
- Manually provided: Human sensors provide the context information [43].

### 2.4. Capabilities

The *capabilities* category contains three dimensions or subcategories (communication, processing, and storage) and refers to the processing power and storage capacity of the underlying technologies and communication protocols. Each dimension has its specific sub-dimensions or characteristics, as represented in Figure 6.

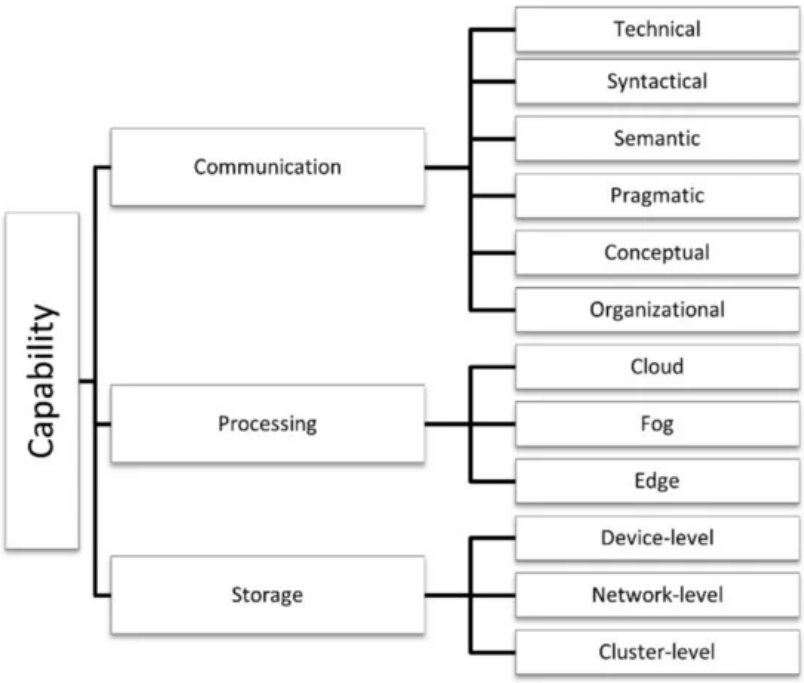


**Figure 6.** IoE Taxonomy: capability category, its dimensions, and characteristics.

#### 2.4.1. Communication

The communication capability refers to the sensors' ability to communicate and change information locally. This ability may vary at different levels of interoperability between IoE sensors and systems and be classified as no connection (no connectivity between enablers), technical (basic network connectivity), syntactical (basic interoperability and data exchange), semantic (understanding about the semantics of the data), pragmatic or dynamic (applicability of the information), conceptual (shared view of the pervasive world) [27], or organizational (coordination and alignment of business processes across organizational boundaries) [119]. Additionally, based on communication capabilities, IoT devices are classified into two categories: gateway devices and constrained devices [103][86]. Moreover, according to their abilities to interact with other objects, IoT objects can be classified into four levels (Level 0–Level 3). Level 0 objects only receive, and Level 1 objects only send information. Level 2 objects can perform both operations with one object, while Level 3 extends the interaction to any other object [61].

Different networking protocols and technologies provide networking interoperability in IoT [27][109][82]. IoT systems can exploit several types of networks with different characteristics in terms of size, data transfer, coverage, latency requirements, capacity, and supported reachability [67][64][110][102][74]. The central networking and communication technologies are local area networks, wireless local area networks, wireless personal area networks, wide area networks, metropolitan area networks, wireless regional area networks, body area networks, mobile communication networks, wireless metropolitan area networks, satellite networks (e.g., GPS) [24][95][120], Neul, IPv6 over low-power personal area networks (6LowPAN), low-range wireless area networks, cellular Sigfox, narrowband-IoT, and thread or mesh technologies such as Zigbee and SDNs [25][30][81].

There are three types of communication protocol that enable IoT to interconnect and communicate: (1) device-to-device, which is applied to communication between mobile phones within reach and is the next-generation of mobile networks; (2) device to the server, in which the sensed data are sent to the servers, nearby or away from devices (applies to cloud processing); and (3) server-to-server, in which servers transmit data between each other—mainly used for mobile networks [52].

#### 2.4.2. Processing

The sensors and devices used for data collection also vary in their processing capabilities [121]. The study of Mon et al. [118] classifies sensors as high-end or low-end devices, depending on resources and computational capabilities. Low-end devices are resource-constrained with regard to energy, processing power, and communication capacities. The processing capability refers to the sensors' ability to process aggregated data locally [84].

For IoE systems, data are automatically processed to deduce knowledge and generate actionable insights. In general, data processing techniques are either historical or proactive. Historical data processing is related to knowledge discovery, whereas proactive data processing provides predictive and actionable insights [24]. A broad category of applications participates in the continuous generation and analysis of high-volume heterogeneous stream data. Next-generation applications will be developed to handle the data in streaming mode and on-the-fly as the value of data resides in its real-time processing [122].

Analytics technology refers to the systematic computational analysis of transforming a variety of data from different sources into information [60] and applying data fusion and mining techniques [45] to make intelligent decisions at the following distribution levels: (1) the device level, where devices are responsible for storage and computing process; (2) the network level, which demands remote communication to fog computing nodes (hubs, base stations, gateways, routers, and servers); and (3) cloud level, which demands remote communication within a group of interconnected servers [24][123][63][82][95].

Cloud, edge and fog computing are critical aspects of the centralized and decentralized IoE environment, considering that devices that have restricted compute and memory capacity need to delegate these functions [25][26][29]. Integrated with cloud computing, edge computing can efficiently address the processing problems related to edge big data. Since in the edge computing paradigm, the data are at the edge of the network [28][89].

A variety of cloud computing and edge computing paradigms are mobile cloud computing, mobile edge computing, and fog computing [32][71][117]. Cloudlets, mobile edge computing, and fog computing are edge computing technologies and rely on virtualization, while mobile cloud computing processes the data of mobile applications at a remote cloud data center.

#### 2.4.3. Storage

This capability refers to an IoE system's storage function, based on the paradigm where its storage function resides: cloud, fog, or edge [63]. A storage platform (public, virtual, or private) offers the flexibility and scalability that an IoE application needs, from development to deployment [29]. Storage refers to storing data internally, and it varies intensively

from one object to another [84]. Storage interactions between IoE enablers may be distinguished significantly depending on the object's storage capabilities. Some objects may have restricted capabilities and store minimum information [124]. Most mobile devices at the edge of the network are resource-constrained in terms of storage, computation capability and battery life [89]. Although almost all of the objects have the capacity to store embedded codes to function internally, they differ in storing aggregated and processed data [59]. An object's storage should also be based on the sensitivity of the information stored [84].

Analytics processing requires real-time data stream processing for supporting the rate of data arrival, data management, and data storage [60] at diverse distribution levels.

Depending on the storage and compute capabilities, the storage capability of an IoE node or application is [82]:

- Device-level: devices are participants in the storage and compute process;
- Network-level: the storage process uses remote connections to fog computing nodes;
- Cluster level: storage function is provided between a set of interconnected servers [82].

## References


1. Evans, D. The Internet of Everything: How More Relevant and Valuable Connections Will Change the World. Available online: https://www.cisco.com/web/about/ac79/docs/innov/IoE.pdf.comiweb/aboutlac79/docs/innov/IoE.pdf (accessed on 8 September 2020).
2. Charmonman, S.; Mongkhonvanit, P. Special Consideration for Big Data in IoE or Internet of Everything. In Proceedings of the 13th International Conference on ICT and Knowledge Engineering (ICT and Knowledge Engineering 2015), Bangkok, Thailand, 18–20 November 2015; pp. 147–150.
3. Yu, J.; Kwon, S.; Kang, H.; Kim, S.; Bae, J.; Pyo, C. A Framework on Semantic Thing Retrieval Method in IoT and IoE Environment. In Proceedings of the International Conference on Platform Technology and Service, Jeju, Korea, 29–31 January 2018; pp. 1–6.
4. Auger, A.; Exposito, E.; Lochin, E. Towards the Internet of Everything: Deployment Scenarios for a QoO-Aware Integration Platform. In Proceedings of the IEEE 4th World Forum Internet Things, Singapore, 5–8 February 2018; pp. 499–504.
5. Xu, G.; Shi, Y.; Sun, X.; Shen, W. Internet of Things in Marine Environment Monitoring: A Review. Sensors 2019, 19, 1711.
6. Srinivas, K.; Jabbar, M.A.; Neeraja, K.S. Sensors in IoE: A Review. Int. J. Eng. Technol. 2018, 7, 158.
7. Di Martino, B.; Li, K.-C.; Yang, L.T.; Esposito, A. Internet of Everything: Algorithms, Methodologies, Technologies and Perspectives; Springer: Singapore, 2018; ISBN 978-981-10-5860-8.
8. Vaya, D.; Hadpawat, T. Internet of Everything (IoE): A New Era of IoT. In ICCCE 2019; Lecture Notes in Electrical Engineering; Springer: Singapore, 2020; Volume 570, pp. 1–6.
9. Bojanova, I.; Hurlburt, G.; Voas, J. Imagineering an Internet of Anything. Computer—IEEE Comput. Soc. 2014, 47, 72–77.
10. Fiaidhi, J.; Mohammed, S. Internet of Everything as a Platform for Extreme Automation. IT Prof. 2019, 21, 21–25.
11. Miraz, M.H.; Ali, M.; Excell, P.S.; Picking, R. Internet of Nano-Things, Things and Everything: Future Growth Trends. Future Internet 2018, 10, 68.
12. Srinivasan, C.R.; Rajesh, B.; Saikalyan, P.; Premsagar, K.; Yadav, E.S. A Review on the Different Types of Internet of Things (IoT). J. Adv. Res. Dyn. Control Syst. 2019, 11, 6.
13. Raj, A.; Prakash, S. Internet of Everything: A Survey Based on Architecture, Issues and Challenges. In Proceedings of the 5th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering, Gorakhpur, India, 2–4 November 2018; pp. 1–6.
14. Ghosh, A.; Chakraborty, D.; Law, A. Artificial Intelligence in Internet of Things. CAAI Trans. Intell. Technol. 2018, 3, 208–218.
15. Langley, D.J.; van Doorn, J.; Ng, I.C.L.; Stieglitz, S.; Lazovik, A.; Boonstra, A. The Internet of Everything: Smart Things and Their Impact on Business Models. J. Bus. Res. 2020, 122, 853–863.

16. Miraz, M.H.; Ali, M.; Excell, P.S.; Picking, R. A Review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT). In Proceedings of the Internet Technologies and Applications, Wrexham, UK, 8–11 September 2015; pp. 219–224.
17. Masoud, M.; Jaradat, Y.; Manasrah, A.; Jannoud, I. Sensors of Smart Devices in the Internet of Everything (IoE) Era: Big Opportunities and Massive Doubts. J. Sens. 2019, 2019, 1–26.
18. Vandebroek, S.V. 1, 2 Three Pillars Enabling the Internet of Everything: Smart Everyday Objects Information-Centric Networks, and Automated Real-Time Insights. In Proceedings of the IEEE International Solid-State Circuits Conference, San Francisco, CA, USA, 31 January–4 February 2016; pp. 14–20.
19. Majeed, A. Developing Countries and Internet-of-Everything (IoE). In Proceedings of the IEEE 7th Annual Computing and Communication Workshop and Conference, Las Vegas, NV, USA, 9–11 January 2017; pp. 1–4.
20. Nonaka, I.; Toyama, R. The Knowledge-Creating Theory Revisited: Knowledge Creation as a Synthesizing Process. In The Essentials of Knowledge Management; Palgrave Macmillan: London, UK, 2015; pp. 95–110.
21. Di Martino, B.; Li, K.-C.; Yang, L.T.; Esposito, A. Trends and Strategic Researches in Internet of Everything. In Internet of Everything; Internet of Things; Di Martino, B., Li, K.-C., Yang, L.T., Esposito, A., Eds.; Springer: Singapore, 2018; pp. 1–12. ISBN 978-981-10-5860-8.
22. Roy, S.; Chowdhury, C. Integration of Internet of Everything (IoE) with Cloud. In Beyond the Internet of Things; Internet of Things; Batalla, J.M., Mastorakis, G., Mavromoustakis, C.X., Pallis, E., Eds.; Springer International Publishing: Cham, Germany, 2017; pp. 199–222. ISBN 978-3-319-50756-9.
23. Jennex, M.E. Big Data, the Internet of Things, and the Revised Knowledge Pyramid. SIGMIS Database 2017, 48, 69–79.
24. Alkhabbas, F.; Spalazzese, R.; Davidsson, P. Characterizing Internet of Things Systems through Taxonomies: A Systematic Mapping Study. Internet Things 2019, 7, 100084.
25. Yaqoob, I.; Ahmed, E.; Hashem, I.A.T.; Ahmed, A.I.A.; Gani, A.; Imran, M.; Guizani, M. Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges. IEEE Wirel. Commun. 2017, 24, 10–16.
26. Mountrouidou, X.; Billings, B.; Mejia-Ricart, L. Not Just Another Internet of Things Taxonomy: A Method for Validation of Taxonomies. Internet Things 2019, 6, 100049.
27. Noura, M.; Atiquzzaman, M.; Gaedke, M. Interoperability in Internet of Things: Taxonomies and Open Challenges. Mob. Netw. Appl. 2019, 24, 796–809.
28. Eris, O.; Drury, J.; Ercolini, D. A Collaboration-Focused Taxonomy of the Internet of Things. In Proceedings of the IEEE 2nd World Forum on Internet of Things, Milan, Italy, 14–16 December 2015; pp. 29–34.
29. Smutný, P. Different Perspectives on Classification of the Internet of Things. In Proceedings of the 17th International Carpathian Control Conference, Tatranska Lomnica, Slovakia, 29 May–1 June 2016; pp. 692–696.
30. Sinche, S.; Raposo, D.; Armando, N.; Rodrigues, A.; Boavida, F.; Pereira, V.; Silva, J.S. A Survey of IoT Management Protocols and Frameworks. IEEE Commun. Surv. Tutor. 2019, 22, 1168–1190.
31. Younis, M. Internet of Everything and Everybody: Architecture and Service Virtualization. Comput. Commun. 2018, 131, 66–72.
32. Nezami, Z.; Zamanifar, K. Internet of Things/Internet of Everything: Structure and Ingredients. IEEE Potentials 2019, 38, 12–17.
33. Al-Emran, M.; Mezhuyev, V.; Kamaludin, A.; Shaalan, K. The Impact of Knowledge Management Processes on Information Systems: A Systematic Review. Int. J. Inf. Manag. 2018, 43, 173–187.
34. Philip, J. An Application of the Dynamic Knowledge Creation Model in Big Data. Technol. Soc. 2018, 54, 120–127.
35. Nickerson, R.C.; Varshney, U.; Muntermann, J. A Method for Taxonomy Development and Its Application in Information Systems. Eur. J. Inf. Syst. 2013, 22, 336–359.
36. Kotis, K.I.; Vouros, G.A.; Spiliotopoulos, D. Ontology Engineering Methodologies for the Evolution of Living and Reused Ontologies: Status, Trends, Findings and Recommendations. Knowl. Eng. Rev. 2020, 35.
37. Bajaj, G.; Agarwal, R.; Singh, P.; Georgantas, N.; Issarny, V. 4W1H in IoT Semantics. IEEE Access 2018, 6, 65488–65506.
38. Bajaj, G.; Agarwal, R.; Singh, P.; Georgantas, N.; Issarny, V. A Study of Existing Ontologies in the IoT-Domain. arXiv 2017, arXiv:1707.00112, 1–24.
39. Bisdikian, C.; Kaplan, L.M.; Srivastava, M.B. On the Quality and Value of Information in Sensor Networks. ACM Trans. Sen. Netw. 2013, 9, 1–26.

40. De Matos, E.; Amaral, L.A.; Hessel, F. Context-Aware Systems: Technologies and Challenges in Internet of Everything Environments. In Beyond the Internet of Things; Internet of Things; Batalla, J.M., Mastorakis, G., Mavromoustakis, C.X., Pallis, E., Eds.; Springer International Publishing: Cham, Germany, 2017; pp. 1–25. ISBN 978-3-319-50756-9.
41. Pozza, R.; Nati, M.; Georgoulas, S.; Moessner, K.; Gluhak, A. Neighbor Discovery for Opportunistic Networking in Internet of Things Scenarios: A Survey. IEEE Access 2015, 3, 1101–1131.
42. Shahid, N.; Aneja, S. Internet of Things: Vision, Application Areas and Research Challenges. In Proceedings of the International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), Palladam, India, 10–11 February 2017; pp. 583–587.
43. Perera, C.; Zaslavsky, A.; Christen, P.; Georgakopoulos, D. Context Aware Computing for The Internet of Things: A Survey. IEEE Commun. Surv. Tutor. 2014, 16, 414–454.
44. Ge, M.; Bangui, H.; Buhnova, B. Big Data for Internet of Things: A Survey. Future Gener. Comput. Syst. 2018, 87, 601–614.
45. Ur Rehman, M.H.; Liew, C.S.; Wah, T.Y.; Khan, M.K. Towards Next-Generation Heterogeneous Mobile Data Stream Mining Applications: Opportunities, Challenges, and Future Research Directions. J. Netw. Comput. Appl. 2017, 79, 1–24.
46. Bonte, P.; Tommasini, R.; De Turck, F.; Ongenae, F.; Valle, E.D. C-Sprite: Efficient Hierarchical Reasoning for Rapid RDF Stream Processing. In Proceedings of the 13th ACM International Conference on Distributed and Event-based Systems—DEBS '19, Darmstadt, Germany, 24–28 June 2019; pp. 103–114.
47. Prat, N. A Hierarchical Model for Knowledge Management. In Encyclopedia of Knowledge Management; IGI Global: Hershey, PA, USA, 2011; pp. 376–388. ISBN 978-1-59904-931-1.
48. Ein-Dor, P. Taxonomies of Knowledge. In Encyclopedia of Knowledge Management, 2nd ed.; IGI Global: Hershey, PA, USA, 2011; pp. 1490–1499.
49. Perera, C.; Vasilakos, A.V. A Knowledge-Based Resource Discovery for Internet of Things. Knowledge-Based Syst. 2016, 109, 122–136.
50. Obinikpo, A.A.; Kantarci, B. Big Sensed Data Meets Deep Learning for Smarter Health Care in Smart Cities. J. Sens. Actuator Netw. 2017, 6, 26.
51. Chaochaisit, W.; Bessho, M.; Koshizuka, N.; Sakamura, K. Human Localization Sensor Ontology: Enabling OWL 2 DL-Based Search for User's Location-Aware Sensors in the IoT. In Proceedings of the IEEE Tenth International Conference on Semantic Computing, Laguna Hills, CA, USA, 4–6 February 2016; pp. 107–111.
52. Mahdavinejad, M.; Rezvan, M.; Barekatain, M. Machine Learning for Internet of Things Data Analysis: A Survey. Digit. Commun. Netw. 2018, 4, 161–175.
53. Grant, J.; Parisi, F. Logic and Knowledge Bases. In Encyclopedia of Knowledge Management, 2nd ed.; Schwartz, D., Ed.; IGI Global: Hershey, PA, USA, 2010; ISBN 978-1-59904-931-1.
54. Höller, J.; Tsiatsis, V.; Mulligan, C. Toward a Machine Intelligence Layer for Diverse Industrial IoT Use Cases. IEEE Intell. Syst. 2017, 32, 64–71.
55. Ruta, M.; Scioscia, F.; Loseto, G.; Pinto, A.; Di Sciascio, E. Machine Learning in the Internet of Things: A Semantic-Enhanced Approach. Semant. Web 2018, 10, 183–204.
56. Qanbari, S.; Behinaein, N.; Rahimzadeh, R.; Dustdar, S. Gatica: Linked Sensed Data Enrichment and Analytics Middleware for IoT Gateways. In Proceedings of the 3rd International Conference on Future Internet of Things and Cloud, Rome, Italy, 24–26 August 2015; pp. 38–43.
57. Damiani, E. Toward Big Data Risk Analysis. In Proceedings of the IEEE International Conference on Big Data, Santa Clara, CA, USA, 29 October–1 November 2015; pp. 1905–1909.
58. Yebda, T.; Benois-Pineau, J.; Amieva, H.; Frolicher, B. Multi-Sensing of Fragile Persons for Risk Situation Detection: Devices, Methods, Challenges. In Proceedings of the International Conference on Content-Based Multimedia Indexing, Dublin, Ireland, 4–6 September 2019; pp. 1–6.
59. Pal, D.; Vanijja, V.; Varadarajan, V. Quality Provisioning in the Internet of Things Era: Current State and Future Directions. In Proceedings of the 10th International Conference on Advances in Information Technology, Bangkok, Thailand, 10–13 December 2018; pp. 1–7.
60. Mohamed, A.; Najafabadi, M.K.; Wah, Y.B.; Zaman, E.A.K.; Maskat, R. The State of the Art and Taxonomy of Big Data Analytics: View from New Big Data Framework. Artif. Intell. Rev. 2019.
61. Bugeja, J.; Davidsson, P.; Jacobsson, A. Functional Classification and Quantitative Analysis of Smart Connected Home Devices. In Proceedings of the Global Internet of Things Summit, Bilbao, Spain, 4–6 June 2018; pp. 1–6.

62. Marjani, M.; Nasaruddin, F.; Gani, A.; Karim, A.; Hashem, I.A.T.; Siddiqa, A.; Yaqoob, I. Big IoT Data Analytics: Architecture, Opportunities, and Open Research Challenges. IEEE Access 2017, 5, 5247–5261.

63. Yaqoob, I.; Hashem, I.A.T.; Gani, A.; Mokhtar, S.; Ahmed, E.; Anuar, N.B.; Vasilakos, A.V. Big Data: From Beginning to Future. Int. J. Inf. Manag. 2016, 36, 1231–1247.

64. Gao, J.; Lei, L.; Yu, S. Big Data Sensing and Service: A Tutorial. In Proceedings of the IEEE First International Conference on Big Data Computing Service and Applications, Redwood City, CA, USA, 30 March–2 April 2015; pp. 79–88.

65. Atat, R.; Liu, L.; Wu, J.; Li, G.; Ye, C.; Yang, Y. Big Data Meet Cyber-Physical Systems: A Panoramic Survey. IEEE Access 2018, 6, 73603–73636.

66. Cai, S.; Gallina, B.; Nyström, D.; Seceleanu, C. Data Aggregation Processes: A Survey, a Taxonomy, and Design Guidelines. Computing 2018, 1–33.

67. Shah, S.A.; Seker, D.Z.; Hameed, S.; Draheim, D. The Rising Role of Big Data Analytics and IoT in Disaster Management: Recent Advances, Taxonomy and Prospects. IEEE Access 2019, 7, 54595–54614.

68. Haron, N.; Jaafar, J.; Aziz, I.A.; Hassan, M.H.; Shapiai, M.I. Data Trustworthiness in Internet of Things: A Taxonomy and Future Directions. In Proceedings of the IEEE Conference on Big Data and Analytics, Kuching, Malaysia, 16–17 November 2017; pp. 25–30.

69. Asghari, P.; Rahmani, A.M.; Javadi, H.H.S. Service Composition Approaches in IoT: A Systematic Review. J. Netw. Comput. Appl. 2018, 120, 61–77.

70. Jing, Q.; Vasilakos, A.V.; Wan, J.; Lu, J.; Qiu, D. Security of the Internet of Things: Perspectives and Challenges. Wirel. Netw. 2014, 20, 2481–2501.

71. Hassan, N.; Gillani, S.; Ahmed, E.; Yaqoob, I.; Imran, M. The Role of Edge Computing in Internet of Things. IEEE Commun. Mag. 2018, 56, 110–115.

72. Ahad, A.; Tahir, M.; Yau, K.-L.A. 5G-Based Smart Healthcare Network: Architecture, Taxonomy, Challenges and Future Research Directions. IEEE Access 2019, 7, 100747–100762.

73. Asghari, P.; Rahmani, A.M.; Javadi, H.H.S. Internet of Things Applications: A Systematic Review. Comput. Netw. 2019, 148, 241–261.

74. Barker, L.; White, M.; Patoli, Z.; Huggins, B.; Pascu, T.; Curran, M.; Beloff, N. Taxonomy for Internet of Things—Tools for Monitoring Personal Effects. In Proceedings of the 4th International Conference on Pervasive and Embedded Computing and Communication Systems, Lisbon, Portugal, 7–9 January 2014; Volume 1, pp. 67–71.

75. Botta, A.; de Donato, W.; Persico, V.; Pescapé, A. Integration of Cloud Computing and Internet of Things: A Survey. Future Gener. Comput. Syst. 2016, 56, 684–700.

76. Ashraf, Q.M.; Habaebi, M.H. Autonomic Schemes for Threat Mitigation in Internet of Things. J. Netw. Comput. Appl. 2015, 49, 112–127.

77. Phuttharak, J.; Loke, S.W. A Review of Mobile Crowdsourcing Architectures and Challenges: Toward Crowd-Empowered Internet-of-Things. IEEE Access 2019, 7, 304–324.

78. Neshenko, N.; Bou-Harb, E.; Crichigno, J.; Kaddoum, G.; Ghani, N. Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations. IEEE Commun. Surv. Tutor. 2019, 21, 2702–2733.

79. Bamgboye, O.; Liu, X.; Cruickshank, P. Towards Modelling and Reasoning About Uncertain Data of Sensor Measurements for Decision Support in Smart Spaces. In Proceedings of the IEEE 42nd Annual Computer Software and Applications Conference, Tokyo, Japan, 23–27 July 2018; pp. 744–749.

80. Chen, C.; Helal, S. A Device-Centric Approach to a Safer Internet of Things. In Proceedings of the International Workshop on Networking and Object Memories for the Internet of Things, Beijing, China, 18 September 2011; pp. 1–6.

81. Boyes, H.; Hallaq, B.; Cunningham, J.; Watson, T. The Industrial Internet of Things (IIoT): An Analysis Framework. Comput. Ind. 2018, 101, 1–12.

82. Siow, E.; Tiropanis, T.; Hall, W. Analytics for the Internet of Things: A Survey. ACM Comput. Surv. 2018, 51, 1–36.

83. Chellappan, V.; Sivalingam, K.M. Security and privacy in the Internet of Things. In Internet of Things—Principles and Paradigms; Morgan Kaufmann: Burlington, MA, USA, 2016; pp. 183–200. ISBN 978-0-12-805395-9.

84. Alsamani, B.; Lahza, H. A Taxonomy of IoT: Security and Privacy Threats. In Proceedings of the International Conference on Information and Computer Technologies, DeKalb, IL, USA, 23–25 March 2018; pp. 72–77.

85. Bellavista, P.; Berrocal, J. A Survey on Fog Computing for the Internet of Things. Pervasive Mob. Comput. 2019, 52, 71–99.

86. Fortino, G.; Rovella, A.; Russo, W.; Savaglio, C. On the Classification of Cyberphysical Smart Objects in the Internet of Things. In Proceedings of the International Workshop on Networks of Cooperating Objects for Smart Cities 2014 (UBICITEC 2014), Berlin, Germany, 14 April 2014; Volume 1156, pp. 86–94.

87. Sholla, S.; Naaz, R.; Chishti, M.A. Ethics Aware Object Oriented Smart City Architecture. China Commun. 2017, 14, 160–173.

88. Abbas, N.; Zhang, Y.; Taherkordi, A.; Skeie, T. Mobile Edge Computing: A Survey. IEEE Internet Things J. 2018, 5, 450–465.

89. Zhang, J.; Chen, B.; Zhao, Y.; Cheng, X.; Hu, F. Data Security and Privacy-Preserving in Edge Computing Paradigm: Survey and Open Issues. IEEE Access 2018, 6, 18209–18237.

90. Sahinel, D.; Akpolat, C.; Gorur, O.C.; Sivrikaya, F. Integration of Human Actors in IoT and CPS Landscape. In Proceedings of the IEEE 5th World Forum on Internet of Things, Limerick, Ireland, 15–18 April 2019; pp. 485–490.

91. Oteafy, S.M.A.; Hassanein, H.S. Leveraging Tactile Internet Cognizance and Operation via IoT and Edge Technologies. Proc. IEEE 2019, 107, 364–375.

92. Oberländer, A.M.; Röglinger, M.; Rosemann, M.; Kees, A. Conceptualizing Business-to-Thing Interactions—A Sociomaterial Perspective on the Internet of Things. Eur. J. Inf. Syst. 2018, 27, 486–502.

93. Moustaka, V.; Vakali, A.; Anthopoulos, L.G. A Systematic Review for Smart City Data Analytics. ACM Comput. Surv. 2018, 51, 1–41.

94. Russell, S.J.; Norvig, P.; Davis, E. Artificial Intelligence: A Modern Approach, 3rd ed.; Prentice Hall Series in Artificial Intelligence; Prentice Hall: Upper Saddle River, NJ, USA, 2016; ISBN 978-0-13-604259-4.

95. Ahmed, E.; Yaqoob, I.; Gani, A.; Imran, M.; Guizani, M. Internet-of-Things-Based Smart Environments: State of the Art, Taxonomy, and Open Research Challenges. IEEE Wirel. Commun. 2016, 23, 10–16.

96. Armando, N.; Rodrigues, A.; Pereira, V.; Sá Silva, J.; Boavida, F. An Outlook on Physical and Virtual Sensors for a Socially Interactive Internet. Sensors 2018, 18, 2578.

97. Salim, F.; Haque, U. Urban Computing in the Wild: A Survey on Large Scale Participation and Citizen Engagement with Ubiquitous Computing, Cyber Physical Systems, and Internet of Things. Int. J. Hum. Comput. Stud. 2015, 81, 31–48.

98. Agarwal, R.; Fernandez, D.G.; Elsaleh, T.; Gyrard, A.; Lanza, J.; Sanchez, L.; Georgantas, N.; Issarny, V. Unified IoT Ontology to Enable Interoperability and Federation of Testbeds. In Proceedings of the IEEE 3rd World Forum on Internet of Things, Reston, VA, USA, 12–14 December 2016; pp. 70–75.

99. Naha, R.K.; Garg, S.; Georgakopoulos, D.; Jayaraman, P.P.; Gao, L.; Xiang, Y.; Ranjan, R. Fog Computing: Survey of Trends, Architectures, Requirements, and Research Directions. IEEE Access 2018, 6, 47980–48009.

100. Hui, T.K.L.; Sherratt, R.S. Towards Disappearing User Interfaces for Ubiquitous Computing: Human Enhancement from Sixth Sense to Super Senses. J. Ambient. Intell. Humaniz. Comput. 2017, 8, 449–465.

101. Haller, S.; Serbanati, A.; Bauer, M.; Carrez, F. A Domain Model for the Internet of Things. In Proceedings of the IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, Beijing, China, 20–23 August 2013; pp. 411–417.

102. Berger, S.; Denner, M.-S.; Röglinger, M. The Nature of Digital Technologies—Development of a Multi-Layer Taxonomy. In Proceedings of the Twenty-Sixth European Conference on Information Systems, Portsmouth, UK, 23–28 June 2018; pp. 1–19.

103. Bhatt, S.; Patwa, F.; Sandhu, R. An Access Control Framework for Cloud-Enabled Wearable Internet of Things. In Proceedings of the IEEE 3rd International Conference on Collaboration and Internet Computing, San Jose, CA, USA, 15–17 October 2017; pp. 328–338.

104. Compton, M.; Barnaghi, P.; Bermudez, L.; García-Castro, R.; Corcho, O.; Cox, S.; Graybeal, J.; Hauswirth, M.; Henson, C.; Herzog, A.; et al. The SSN Ontology of the W3C Semantic Sensor Network Incubator Group. J. Web Semant. 2012, 17, 25–32.

105. Rozsa, V.; Denisczwicz, M.; Dutra, M.; Ghodous, P.; Silva, C.F.D.; Moayeri, N.; Biennier, F.; Figay, N. An Application Domain-Based Taxonomy for IoT Sensors. In Transdisciplinary Engineering: Crossing Boundaries, Proceedings of the 23rd ISPE International Conference on Transdisciplinary Engineering: Crossing Boundaries, Curitiba, Brazil, 3–7 October 2016; IOS Press BV: Amsterdam, The Netherlands, 2016; Volume 4, pp. 249–258.

106. Montori, F.; Jayaraman, P.P.; Yavari, A.; Hassani, A.; Georgakopoulos, D. The Curse of Sensing: Survey of Techniques and Challenges to Cope with Sparse and Dense Data in Mobile Crowd Sensing for Internet of Things. Pervasive Mob.

Comput. 2018, 49, 111–125.

107. Ravignani, A.; Olivera, V.; Gingras, B.; Hofer, R.; Hernández, C.; Sonnweber, R.-S.; Fitch, W. Primate Drum Kit: A System for Studying Acoustic Pattern Production by Non-Human Primates Using Acceleration and Strain Sensors. Sensors 2013, 13, 9790–9820.
108. Dorsemaine, B.; Gaulier, J.; Wary, J.; Kheir, N.; Urien, P. Internet of Things: A Definition & Taxonomy. In Proceedings of the 9th International Conference on Next Generation Mobile Applications, Services and Technologies, Cambridge, UK, 9–11 September 2015; pp. 72–77.
109. Sethi, P.; Sarangi, S.R. Internet of Things: Architectures, Protocols, and Applications. J. Electr. Comput. Eng. 2017, 2017, 1–25.
110. Subbu, K.P.; Vasilakos, A.V. Big Data for Context Aware Computing—Perspectives and Challenges. Big Data Res. 2017, 10, 33–43.
111. Taylor, W.; Abbasi, Q.H.; Dashtipour, K.; Ansari, S.; Shah, S.A.; Khalid, A.; Imran, M.A. A Review of the State of the Art in Non-Contact Sensing for COVID-19. Sensors 2020, 20, 5665.
112. Oliveira, L.; Schneider, D.; De Souza, J.; Shen, W. Mobile Device Detection Through WiFi Probe Request Analysis. IEEE Access 2019, 7, 98579–98588.
113. Saad, E.; Elhosseini, M.; Haikal, A.Y. Recent Achievements in Sensor Localization Algorithms. Alex. Eng. J. 2018, 57, 4219–4228.
114. Shit, R.C.; Sharma, S.; Puthal, D.; Zomaya, A.Y. Location of Things (LoT): A Review and Taxonomy of Sensors Localization in IoT Infrastructure. IEEE Commun. Surv. Tutor. 2018, 20, 2028–2061.
115. Abdul-Ghani, H.A.; Konstantas, D.; Mahyoub, M. A Comprehensive IoT Attacks Survey Based on a Building-Blocked Reference Model. Int. J. Adv. Comput. Sci. Appl. 2018, 9.
116. Abbas, S.S.A.; Priya, K.L. Self Configurations, Optimization and Protection Scenarios with Wireless Sensor Networks in IIoT. In Proceedings of the International Conference on Communication and Signal Processing, Chennai, India, 4–6 April 2019; pp. 0679–0684.
117. Nayyer, M.Z.; Raza, I.; Hussain, S.A. A Survey of Cloudlet-Based Mobile Augmentation Approaches for Resource Optimization. ACM Comput. Surv. (CSUR) 2019, 51, 107.
118. Mon, A.; Giorgio, H.R.D.; María, E.D.; Querel, M.; Figuerola, C. Evaluation of Technological Development for the Definition of Industries 4.0. In Proceedings of the Congreso Argentino de Ciencias de la Informática y Desarrollos de Investigación, Buenos Aires, Argentina, 28–30 November 2018; pp. 1–6.
119. Pliatsios, A.; Goumopoulos, C.; Kotis, K. A Review on IoT Frameworks Supporting Multi-Level Interoperability—The Semantic Social Network of Things Framework. Int. J. Adv. Internet Technol. 2020, 13, 46–64.
120. Mehmood, Y.; Ahmad, F.; Yaqoob, I.; Adnane, A.; Imran, M.; Guizani, S. Internet-of-Things-Based Smart Cities: Recent Advances and Challenges. IEEE Commun. Mag. 2017, 55, 16–24.
121. Fan, H.; Li, J.; Chen, N.; Hu, C. Capability Representation Model for Heterogeneous Remote Sensing Sensors: Case Study on Soil Moisture Monitoring. Environ. Model. Softw. 2015, 70, 65–79.
122. Mehmood, E.; Anees, T. Challenges and Solutions for Processing Real-Time Big Data Stream: A Systematic Literature Review. IEEE Access 2020, 8, 119123–119143.
123. Gluhak, A.; Krco, S.; Nati, M.; Pfisterer, D.; Mitton, N.; Razafindralambo, T. A Survey on Facilities for Experimental Internet of Things Research. IEEE Commun. Mag. 2011, 49, 58–67.
124. Uschold, M.; Gruninger, M. Ontologies: Principles, Methods and Applications. Knowl. Eng. Rev. 1996, 11, 93–155.

Retrieved from https://encyclopedia.pub/entry/history/show/16081