Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2018, 5(10): 745-767

Review Article ISSN: 2394 - 658X

The Internet of Things: A Conceptual Guided Tour

Spyros G. Tzafestas

School of Electrical and Computer Engineering, National Technical University of Athens
Zographou 15773, Athens, Greece

ABSTRACT

The Internet of Things (IoT) is an enhancement of the Internet that can be described as things/objects in our environment being connected anytime and anywhere with anything and anyone, over the Internet, so as to give seamless communications and external services. Thus, IoT is a web of a tremendous number of connections of 'things with things', and 'humans with things', which is naturally more dynamic and more complex than the internet itself. The purpose of this article is to provide a summarized conceptual tour to IoT that covers ontological issues, characteristics, advantages and disadvantages, architectures and platforms, hardware and software components, and examples of typical applications.

Key words: Internet of things (IoT), IoT characteristics, IoT architectures, IoT advantages, IoT disadvantages, IoT impacts, IoT applications

---

1. INTRODUCTION

The *Internet of Things* **(IoT)** represents an engineering development in which the Internet extends into the real world embracing everyday objects. Physical entities are no longer disconnected from the virtual world, but can be controlled remotely and can act as physical access points to Internet services. The Internet of Things is a new enhancement of the Internet which aims at enabling 'Things' to be connected *anytime (any context)* at *anyplace (anywhere)* with *anything (any device)* and *anyone* using *any path or network* and *any service or business* (Fig. 1) [1]. The potential of IoT is increased by its proper use for enhancing the insights from data, and for digitizing, automating, optimizing, transforming processes and business models, and even operating industries in a scope of digital transformation.

IoT can provide services to all kinds of applications, while assuring the fulfilment of safety, security and privacy requirements, by exploiting data gathering, identification, processing and communication capabilities. IoT makes, using ICT, infrastructure components and services for smart home, smart office, smart city, smart industry, real estate, healthcare, public safety, and, generally, for more interactive and efficient transportation and power utilities, etc. As many scholars note, IoT will serve as a basis for significant changes in technologies which are planned in the near future. This can be applied to almost all sectors of modern man and society. In this sense IoT can serve as the embodiment of technology and techniques in today's information society. IoT is a network of smart devices that can send and receive information, and make various administrative decisions based on the obtained data. IoT is also a special platform, i.e., a special software and systemic base, through which several applications can be created.

The aim of this article is to provide a short conceptual tour to the IoT world. Specifically, the article:

- Discusses the ontological question: 'what is the Internet of Things', presenting ten alternative definitions.
- Presents the fundamental characteristics/features of IoT.
- Outlines the architectures of IoT including IoT basic architectures, IoT cloud and fog architectures, and IoT reference architectures.
- Discusses the IoT platforms, in general, and the Intel IoT platform, in particular.
- Provides a number of representative IoT application examples.
- Discusses the primary IoT advantages and disadvantages.
- Provides a list of basic IoT hardware components and IoT software applications.

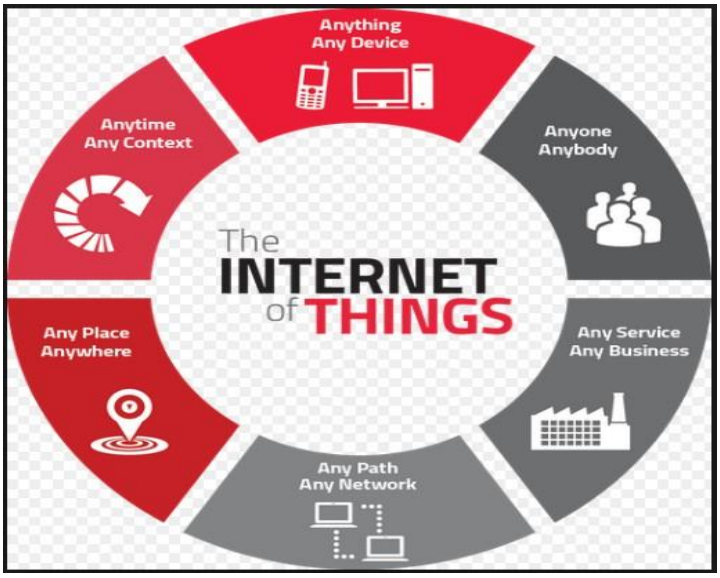


Fig. 1 Interconnections in IoT
Source: https://learninternetgovernance.blogspot.com/p/internet-of-things-iot.html

WHAT IS THE INTERNET OF THINGS?

The term "*Internet of Things"* **(IoT)** is now widely used, but so far there is not a unique common non-biased definition or understanding of what this term encompasses. There are many different definitions of the expression "Internet of Things" which however have in common the feature that it has to do with the integration of the physical world with the virtual world of the internet. These definitions/views depend on how professionals look at it, *viz.* from a technological perspective, an application perspective, an industrial perspective, etc. The phrase *Internet of things* was first used in 1999 by Kevin Ashton, director of Auto-ID Center (MIT), working on networked "*radio-frequency identification"* (**RFID**) infrastructures [1-4]. He coined this term in order to reflect his envisioning of a world in which all electronic devices are networked and every object (physical or electronic) is tagged with information pertinent to that object [2]. As many thinkers note, the IoT does not concern objects only, but also includes the study of the relations between the everyday objects surrounding humans and humans themselves. Clearly, this fact implies that an urgent wide consideration of the philosophy and ethics of IoT is needed in all sectors of the society. The *Internet of things*, which is sometimes referred to as *Internet of Objects* **(IoO),** is actually a new enhancement of the Internet, and the objects make them recognizable by communicating information about them. They can get information about them accumulated by other objects and things, or they can be elements of high-level services.

Actually, IoT is distinguished in three interaction categories [1]:

- People to people IoT.
- People to things (objects, machines) IoT.
- Things/machines to things/machines IoT.

'Things' refer in general to everyday objects that are readable, recognizable, locatable, and addressable via information sensing devices, and/or controllable via the Internet, irrespectively of the communication means employed (RFID, wireless LAN, WAN, etc.).

IoT is interdisciplinary, and according to Atzori *et al.* [2], can be realized in three paradigms:

- Internet-oriented (middleware).
- Things-oriented (sensors).
- Semantic-oriented (knowledge).

It is remarked that IoT is particularly important and useful in application domains that belong to all the above paradigms.

Some representative definitions of IoT are the following:

Definition 1: *(Auto-ID Center RFID Group)*: "IoT is the worldwide network of interconnected objects uniquely addressable based on standard communication protocols" [3, 4].

Definition 2: *(ITU: International Communication Union)*: "IoT is a global infrastructure for the information society enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies" [5].

Definition 3 *(Forrester)*: "IoT is a smart environment that uses ICTs to make critical infrastructure components and services of a city administration, education, healthcare, public safety, real estate, transportation and utilities more aware, interactive, and efficient" [6].
Definition 4 (*IEEE IoT Initiative, 2014*): "An IoT is a network of items-each embedded with sensors-which are connected to the Internet" [7].
Definition 5 (*NIST Global City Teams, 2014*): ''Cyber-physical Systems/CPS, sometimes referred to as the Internet of Things/IoT, involves connecting smart devices and systems in diverse sectors like transportation, energy, manufacturing and health care in fundamentally new ways" [8].
Definition 6 (*IETF /Internet Engineering Task Force, 2010*): "The basic idea is that IoT will connect objects around us (electronic, electrical, non-electrical) to provide seamless communication and contextual services provided by them, Development of RFID tags, sensors, actuators, mobile phones make it possible to materialize IoT which interact and cooperate each other to make the service better and accessible any time, from anywhere" [9].
Definition 7 (*EU FP7 CASAGRAS Final Report*): "IoT is a global network infrastructure, linking physical and virtual objects through the exploitation of data capture and communication capabilities. This infrastructure includes existing and evolving Internet and network developments."[10].
Definition 8 (*HP/Hewlet Packard*): "IoT refers to the unique identification and internetization of everyday objects. This allows for human interaction and control of these things from anywhere in the world, as well as device-to-device interaction without the need for human involvement" [11].
Definition 9 (*IEEE IoT Initiative, 2015*)**:** In a *small environment scenario*, "An IoT is a network that connects uniquely identifiable 'Things' to the Internet. The 'Things' have sensing/actuator and potential programmability capabilities. Through the exploitation of unique identification and sensing, information about the 'Thing' can be collected and the state of the 'Thing' can be changed from anywhere anytime, by anything" [12].
For a *large environment scenario*, where a large number of 'Things" can be interconnected to provide complex services and enable the execution of complex processes, IEEE IoT Initiative defines IoT as follows:
Definition 10 (*IEEE IoT Initiative, 2015*): "Internet of Things envisions a self-configuring, adaptive, complex network that interconnects 'things' to the Internet through the use of standard communication protocols. The interconnected things have physical or virtual representation in the digital world, sensing/actuator capability, a programmability feature, and are uniquely identified. The representation contains information including the thing's identity, status, location or any other business, social or privately relevant information. The things offer services, with or without human intervention, through the exploitation of a unique identification, data capture and communication, and actuation capability. The service is exploited through the use of intelligent interfaces and is made available anywhere, anytime, and for everything taking security in consideration" [12].
It appears that the IEEE definition 10 (which is a more or less description rather than a compact definition) encompasses most features of IoT.
A map that globally represents IoT, including consumer, industrial and government applications, is shown in Fig. 2 [13].

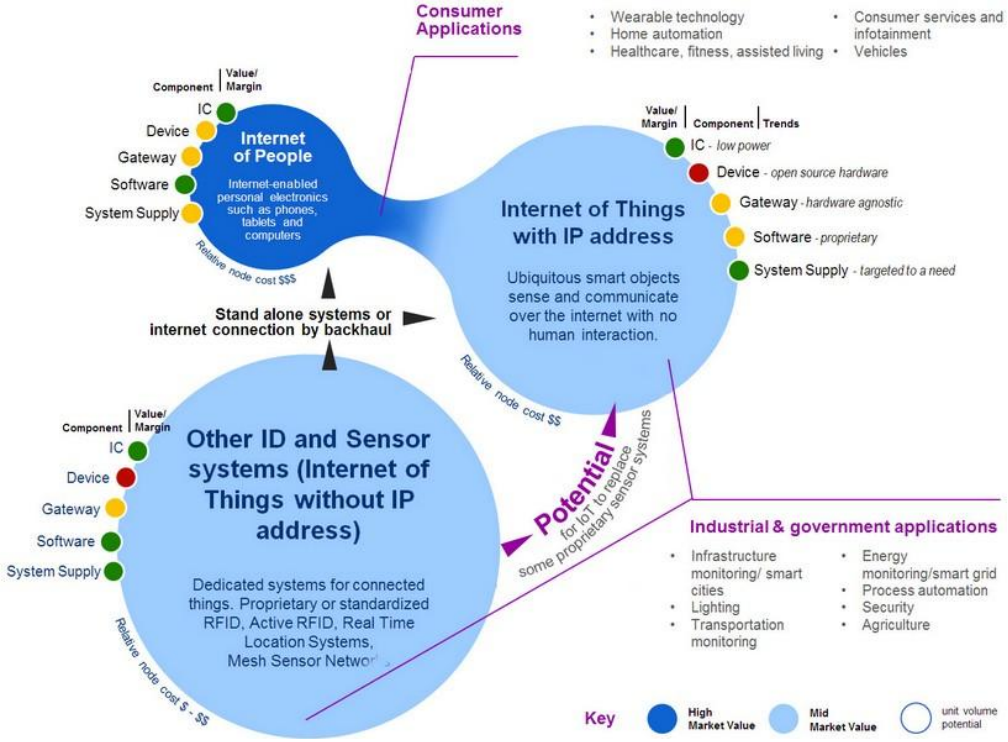


Fig. 2 Overall map of IoT. Source: Internet of Things USA. https://www.i-scoop.eu/internet-of-things-guide/

An alternative term to IoT is the term, *Internet of Everything* **(IoE)**, where the term "Everything" is interpreted as the union of three sets, namely: "Digital", "Things", and "Humans". Therefore, the IoE field involves the three sub-fields *Internet of Digital* **(IoD)**, *Internet of Things* **(IoT)**, and I*nternet of Humans* **(IoH)**, as shown in Fig. 3.

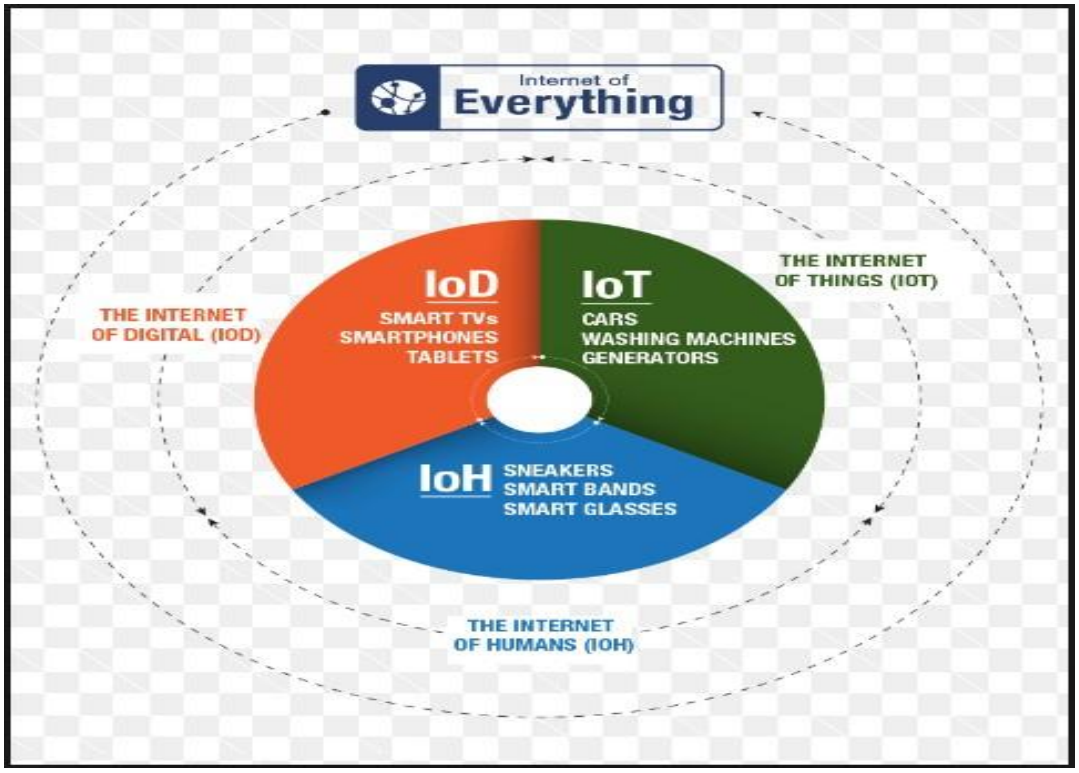


Fig. 3 The three sub-areas of the Internet of Everything (IoE). (a) Internet of Digital (IoD), (b) Internet of Things (IoT), (c) Internet of Humans (IoH). Source: https://www.abiresearch.com/pages/what-is-internet-things/

A set of six application categories (homes, energy, industry, logistics, medical, agriculture) are depicted in Fig. 4.

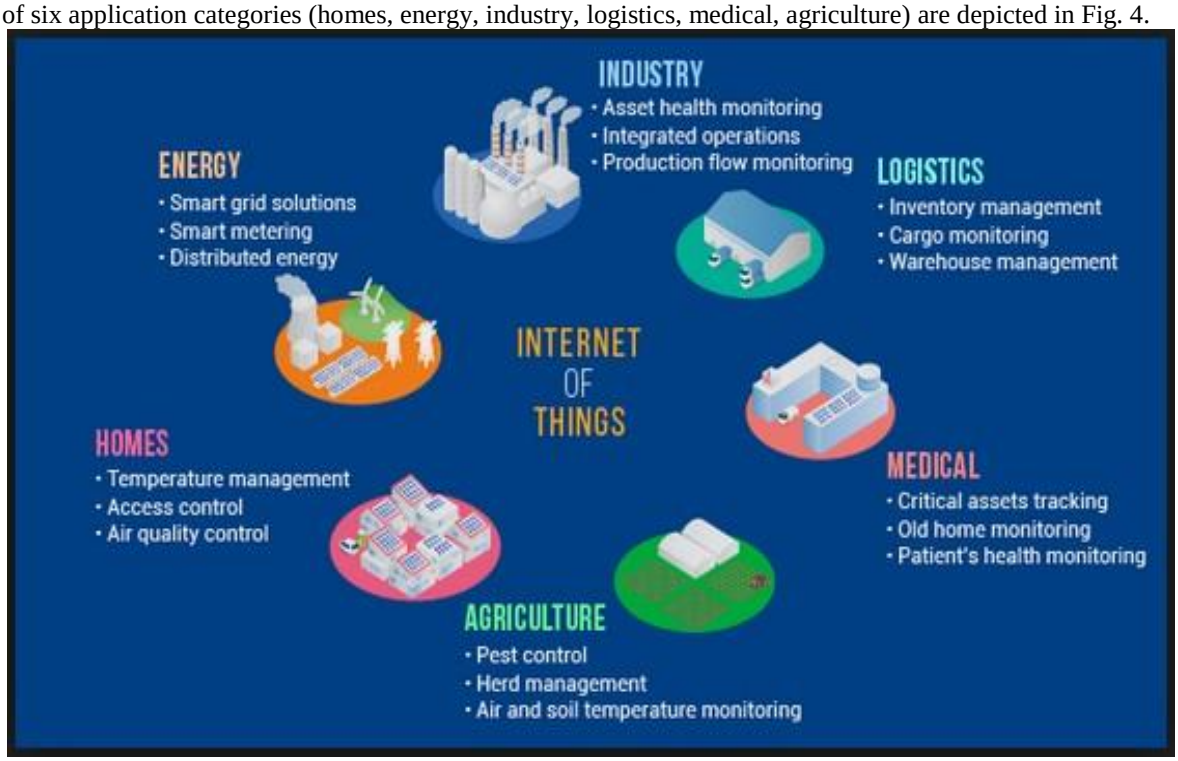


Fig. 4 Six IoT application areas with respective specific cases.
Source: www.powersoft19.com/internet-of-things.html

Internet of Things Characteristics

Here, a short review of the fundamental characteristics of IoT is provided [1, 14].

- ***Connectivity:*** Connectivity makes possible network accessibility and compatibility. Anything can be interconnected with the overall IoT communication and information facilities. Compatibility means that 'things' have the common ability to generate and consume data.
- ***Heterogeneity:*** IoT components and devices are heterogeneous since they are based on different platforms and networks. They can communicate and interact with other devices and service platforms via a variety of networks.
- ***Tremendous scale:*** The IoT number of things and devices that communicate and interact with each other, and have to be managed, is at least one order of magnitude bigger than that of the present internet.
- ***Dynamic changes:*** The state and number of components and devices of IoT change dynamically (e.g., alternating connection and disconnection, changing position and speed, etc.).
- ***Ontological vagueness:*** Human beings, physical objects, and artifacts may not be clearly distinguished due to the deliberate transformation of entities of one type into entities of another type via tagging, engineering, and absorption into a network of artifacts. Criteria to deal with ambiguous identity and system boundary should be developed and used.
- ***Safety:*** IoT should be designed for safety of personal data, physical safety, and human well-being. Securing the end points, the networks, and the data travelling through them, implies that we create a security paradigm that we scale.
- ***Small devices:*** Devices are becoming smaller and smaller, cheaper, and more powerful over time. IoT uses small devices built for several tasks and purposes, to achieve its accuracy, scalability and versatility.
- ***Autonomous agency:*** IoT gives an environment for getting augmented human agency, sometimes reaching the point of spontaneous unexpected interventions that are not directly caused by human beings.
- ***Pervasiveness /ubiquity:*** IoT embeds computational capability into everyday objects and makes them effectively communicate and perform desired tasks in a way that minimizes the human need to interact with computers as computers. IoT devices are network-connected devices and always available. IoT makes computing truly ubiquitous and opens new horizons for the society, the economy, and the individual.
- ***Intelligence:*** IoT has embedded artificial intelligence that enhances every aspect, including smart and dynamic 'things' and knowledge functions as "tools" which constitute extensions to the human body and mind. Actually, IoT enhances every aspect of reality with the abilities of data mining, AI algorithms and features, and networks to achieve accuracy, scalability, and versatility.
- ***Distributed control:*** In IoT the control is not centrally exerted but, because of the enormous number of nodes, it has a distributed form and exhibits emergent features and behaviors which require proper distributed control.
- ***Expressing:*** This feature enables interactivity with people and the physical world. In all cases, *'expressing'* helps us to create products/things that interact intelligently with the real world and the environment.

Internet of Things Architectures

IoT Basic Architectures

Actually, there is not a unique IoT architecture universally agreed. Different architectures were proposed by different researchers and groups. A survey of available IoT architectures and their security protocols is provided in [15]. The most fundamental architecture is the protocol-based 3-layer architecture (Fig. 5). The three layers of this architecture are the following [16]:

Layer 1—*Perception:* This is the physical layer with sensors collecting data/information about the environment.

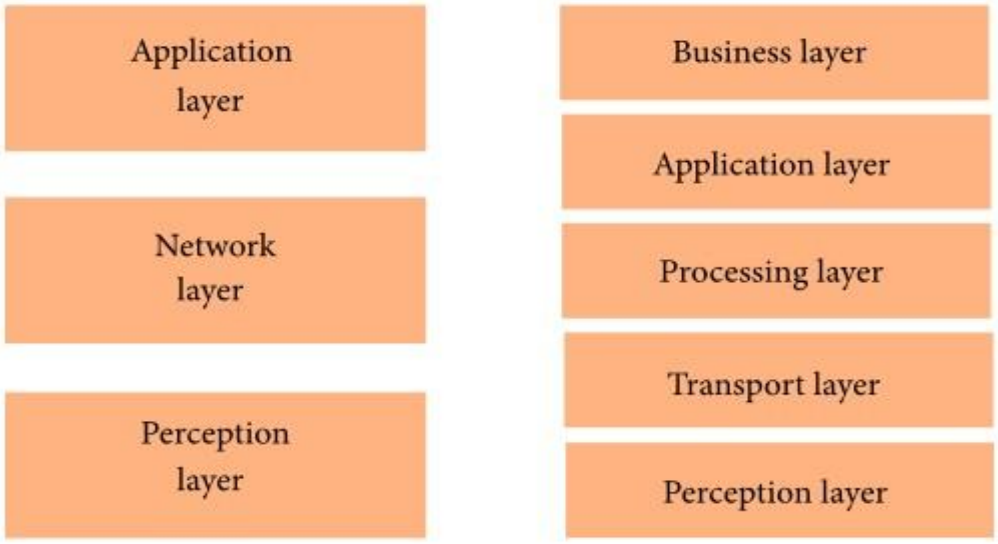
Layer 2—*Network:* This is the layer where the connections to other things, devices and services are realized, and also the sensor data are processed and transmitted.

Layer 3—*Application:* This layer is responsible for defining the applications in which IoT can be deployed, and delivering application specific services to the users.

This 3-layer architecture covers only the basic needs of IoT, but not more detailed features needed for pursuing research in IoT that can be studied using more layers. For example, a 5-layer architecture involves the following layers: *perception, transport, processing, application,* and *business.* The perception and application layers perform the functions indicated above, and the transport, processing, and business layers work as follows:

- ***Transport Layer:*** This layer realizes the bilateral transmission of the sensor data from the perception layer to the processing layer and conversely.
- ***Processing* or *Middleware Layer:*** This layer stores, organizes and processes the large amounts of data received from the transport layer.
- ***Business Layer:*** This layer performs the management of the entire IoT system that involves user's privacy, applications, profit and business processes, etc.

The 3-layer and 5-layer architectures are depicted in Fig. 5.



(a) (b)

Fig. 5 Protocol-based IoT architectures. (a) 3-layer architecture, (b) 5-layer architecture. Source: [16].

In a 7-layer IoT architecture we have the following bottom-up layers: Things layer, Connectivity/Edge computing layer, Global infrastructure layer, Data ingestion layer, Data analysis layer, Applications layer, and People and process layer. The functions performed on these layers are illustrated in Fig. 6.

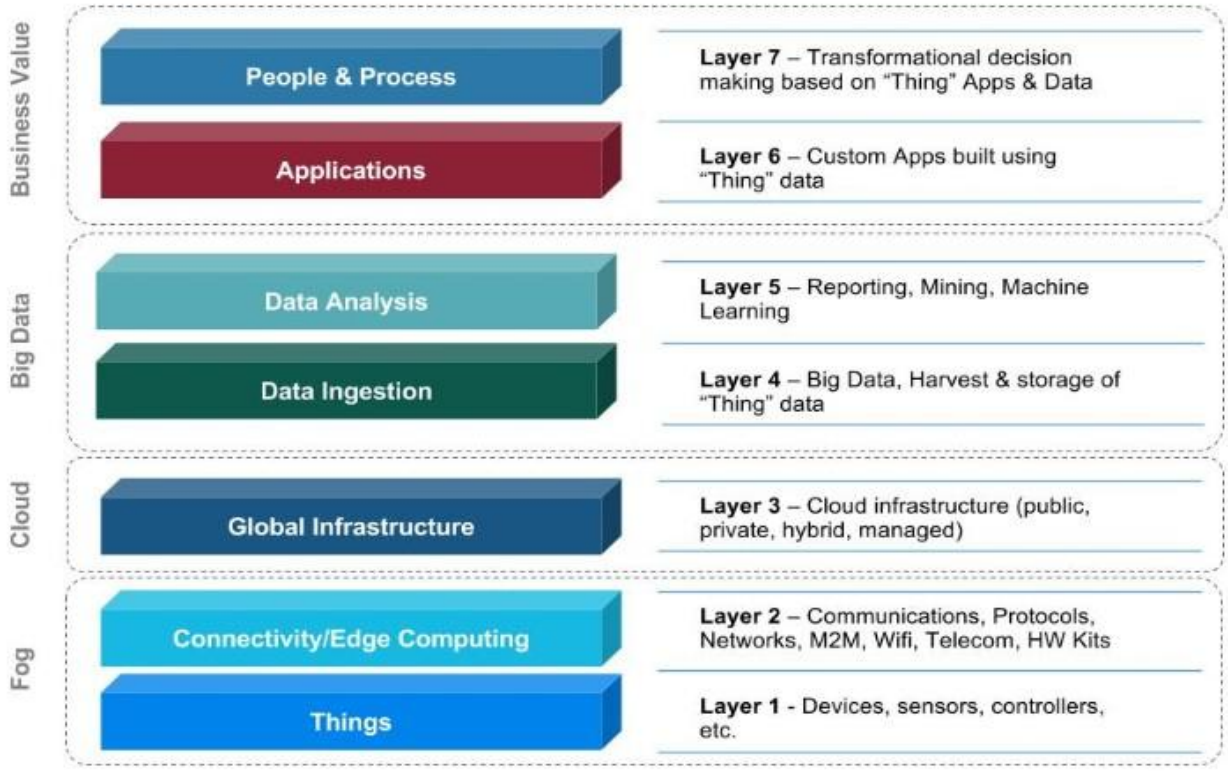


Fig. 6 IoT represented by a seven layer architecture. Source: http://forbes.com/sites/mikekavis/2016/02/24/investors-guide-to-iot-part-1-understanding-the-ecosystem/#63315d726cef, https://www.cloudtp.com/doppler/investors-guide-iot-part-3-iot-platforms-services/, http://iottimes.wordpress.com

IoT Cloud and Fog Architectures

Other architectures include the following:

- ***Cloud Computing Architectures:*** In these architectures the data processing is performed in a large centralized way by cloud computers. Cloud-centric architectures have the cloud at the center, applications above it, and

network of smart things below. Data storage, data mining, software, machine learning, visualization tools, and applications are provided via the cloud (Fig. 7).

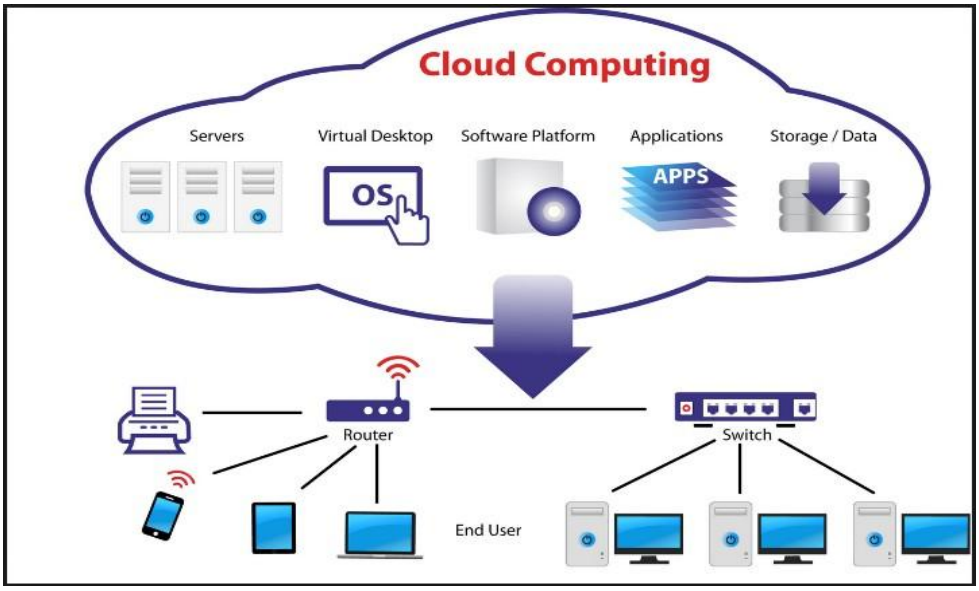


Fig. 7 Typical form of cloud computing architecture
Source: www.educasistemas.com/2018/04/curso-de-cloud-computing-google.html

- ***Fog Computing Architectures:*** Fog computing is an extension of cloud computing to the edge of the network. The goal of *Fog computing* or *Edge computing* is to improve the efficiency of local and cloud data storage. It minimizes the amount of data required to be sent to the cloud which advances data analysis efficiency and the security of IoT. The Fog brings edge devices and the cloud closer together [16, 17]., i.e., although cloud computing operates on the upper layers based mainly on centralized computing, fog computing works on the edge layers and decentralizes the work load at the access points (Fig. 8). In Fog computing environment, a substantial amount of processing may be done in a data hub on the edge of the network in a smart router or other gateway device (e.g. a smart mobile device). Fog works with the cloud, whereas the edge layer excludes the cloud.

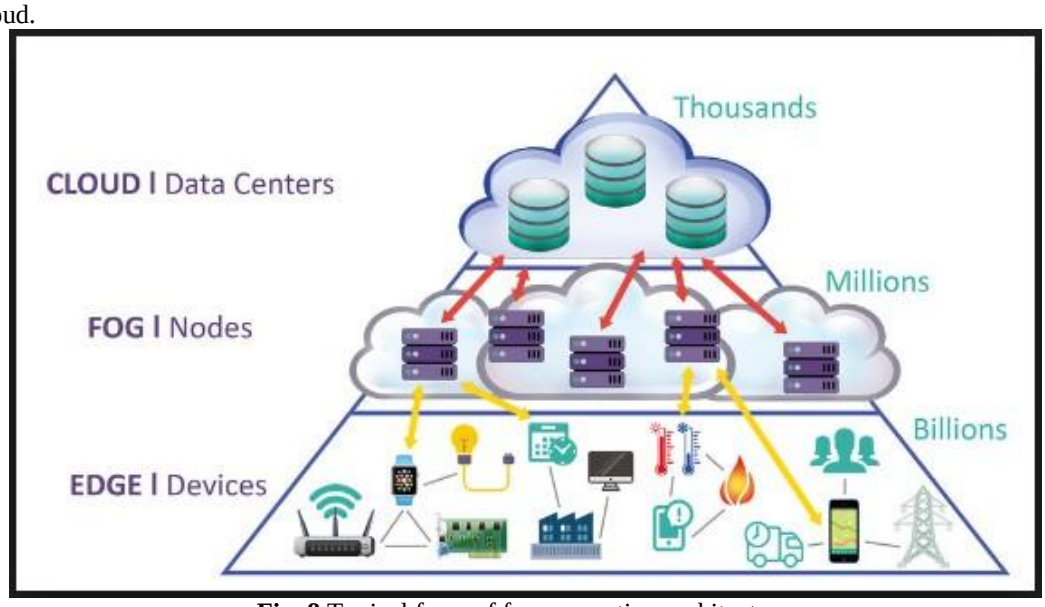


Fig. 8 Typical form of fog computing architecture
Source: www.leanbi.ch/en/blog/iot-and-predictive-analytics-fog-and-edge-computing-for-industries-versus-cloud-19-1-2018/

Fog deals with networking, storage, control, and acceleration, and pushes computing power to the periphery of the network, and is performed for a group of "Things" between Edge and Cloud.
The Fog architecture of a small IoT gate involves between the physical and transport layers in bottom-up hierarchical order the following layers:

- *Monitoring layer* (monitors resources, power, responses and services).
- *Preprocessing layer* (performs filtering, processing, and analytics).
- *Storage layer* (performs storage operations such as data storage, replication and distribution).
- *Security layer* (performs encryption/decryption, and assures data integrity and privacy).

In all cases: ***Devices*** send and receive data interacting with the ***Network,*** in which the data are transmitted, normalized and filtered using ***Edge computing,*** before landing in ***Data bases and storage*** accessible by ***Applications*** which process it and provide it to people who will ***Act and collaborate.***

IoT Reference Architectures

The greatest need for reference architectures is in industry and industrial automation, and so their development and evolution is the result of close cooperation between research and industry. Reference architectures provide guidelines useful for planning the implementation of IoT systems, and therefore help considerably in the standardization of them. Actually, standardization can be achieved through high-level reference architectures which, however, are difficult to be understood because they are very abstract. Therefore, much work has been devoted towards creating concrete less high-level architectures corresponding to various reference architectures, and developing guidelines for doing this. The basic requirements of a generic architecture, like all IoT architectures, are:

- *Data collectionability* (information/knowledge extraction) and analysis tools.
- *Connectivity and communication* (unicast, multicast).
- *Scalability* (capability to adapt to, and process increased data volumes for different system sizes).
- *Security* (trust, privacy).
- *Predictive analysis* (capability to predict events and situations).

Three IoT Reference Architectures are the following [2, 18, 19]:

- **RAMI 4.0:** Reference architecture model industry 4.0 (this architecture is domain specific, and adds to IoT manufacturing and logistic details).
- **IIRA:** Industrial internet reference architecture (the focus of this architecture is on the functionality—monitoring, forecasting, optimization, etc. -- of the industry domain).
- **IoT-A:** Internet of Things Architecture (this architecture concentrates on the generic issues of information, including details of the IoT information technology aspects and provides extensive standardization in M2M communication stacks).

A reference architecture for IoT (**WS02** *Architecture*) is depicted in Fig. 9.

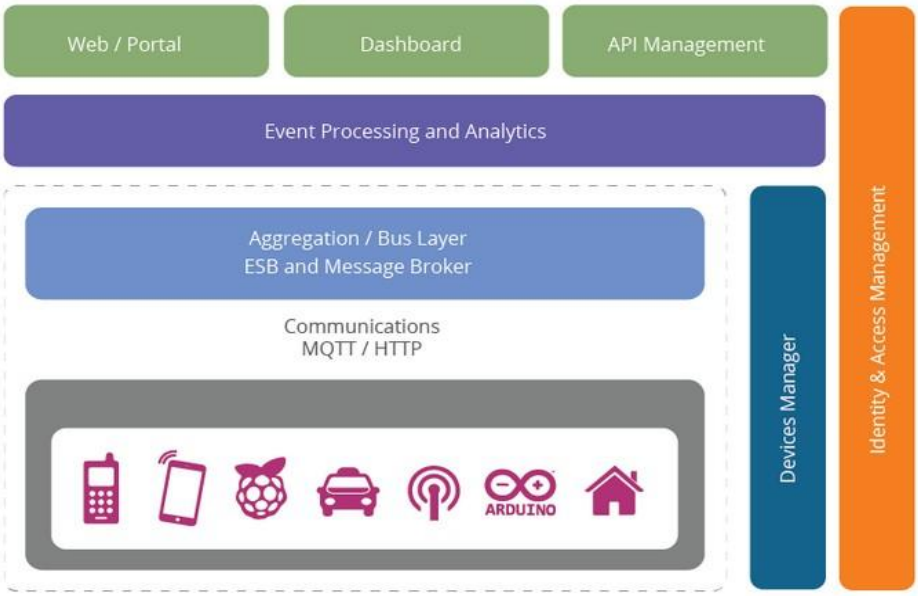


Fig. 9 WS02IoT reference architecture.

Source: https://ws02.com/whitepapers/a-reference-architecture-for-the-internet-of-things/#03

This architecture has the following layers [20]:

Layer 1: Client/external communication—Web/Portal, Dashboard, API's Management.

Layer 2: Event processing and analytics. It provides a complete platform for data analysis with the WS02 Data Analytics server.

Layer 3: Aggregation/bus—ESB and message broker (supports an HTTP/MQTT broker to talk to the devices).

Layer 4: Relevant transports—Protocols MQTT/HTTP/HTTPS/CoAP (Constrained Application Protocol).

This architecture has also the following two crosscutting layers:

1. ***Device management layer:*** A device can be considered an IoT device if it has some communications that directly or indirectly attaches it to the internet (WiFi, Ethernet connection, Bluetooth) having a unique identifier (UID).
2. ***Identity and access management layer*** The WS02 identity server supports this aspect providing several capabilities.

IoT Platforms

IoT platform is an integrated software service system that enables one to bring things to an IoT system, and facilitates data flow, communication, device management, and functionality of applications. Specifically, IoT platforms assist to the following [21, 22]:

- Connect hardware.
- Handle various communication protocols.
- Integrate with other web services.
- Offer security and authentication for things, devices, services, and users.

The three primary kinds of IoT platforms are the following:

- *End-to-end platforms:* They provide hardware and software, connectivity, and handle huge numbers of concurrent devices.
- *Connectivity platforms:* These platforms offer low-cost connectivity via WiFi and cellular methods.
- *Cloud platforms:* They enable us to deal with the complexity of building complex network stacks, also offering additional services (backend services, etc.).

Today there are more than 400 platforms and their number is increasing every year. Some examples of available IoT platforms are the following [21]:

1. **Particle platform:** An enterprise-oriented platform that offers all that one needs to build any IoT product.
2. **Sales force platform:** A platform that maximizes business work with the aid of IoT cloud devices.
3. **Artic cloud platform:** A platform that enables open data exchange for the IoT.
4. **Google Cloud platform:** A platform offering integrated services enabling easy and secure connection, data injection, and management.
5. **Thing Speak platform:** An open IoT platform which can work with MATLAB analytics.
6. **Microsoft Az are IoT:** A platform that enhances the operational productivity and profitability with a connected preconfigured factory.
7. **C3 IoT:** A platform suitable for rapidly developing and using big data, and building advanced applications.

A comparison of four major IoT platforms (GE, Microsoft, Amazon, IBM) is provided in Table 1 [22].

Table -1 Three major IoT platforms compared

Company	**General Electric**	**Microsoft**	**Amazon**	**IBM**
Platform name	Predix	IoT Hub	AWS IoT	IBM Watson IoT
CRM/ERP Integration	Manual	Manual	Manual	Manual
Field Service Integations	ServiceMax	Manual/Partners	Manual/Partners	Manual Partners
Visualization	YES	YES	YES	YES
Analytics-Hot Path	YES	YES	YES	YES
Analytics-Cold Path	YES	YES	YES	YES
Machine Learning	YES	YES/API	YES	
BigData-Hadoop	YES	YES with HD Insight	YES with Amazon EMR	
Notification and Alerts	YES	YES	YES	
Device Lifecycle Mgmt	YES	YES	YES	YES
Device Security	YESX509,	TLSX	509	TLS
Device-Device SDK	YES	Open Source SDK	Open SDK	YES
Device-Protocols	YES	AMQP, MQTT, HTTP	MQTT, HTTP, Web Sockets	MQTT, HTTP
Device-Gateways	YES	YES	YES	YES
Object Storage	YES	YES	YES	YES

The Intel IoT Platform

The *Intel IoT platform* is available in two versions (Version 1.0, Version 2.0) that co-exist and are appropriate for open and scalable solutions.

Version 1.0: ***The Intel IoT Platform for Connecting the Unconnected***

This version specifies how system developers and system integrators can use an IoT gateway to securely connect and manage legacy devices that were not originally built with intelligence or Internet connectivity.

Version 2.0: ***The Intel IoT for Smart Connected things***

This version determines how to integrate a large range of smart and connected things, from simple battery powered things to ultra-high performance devices, that possess intelligence and connectivity already realized.

The architecture of the Intel platform is a 6-layer architecture with an additional vertical security layer which assures world-class security for all layers (Fig. 10).

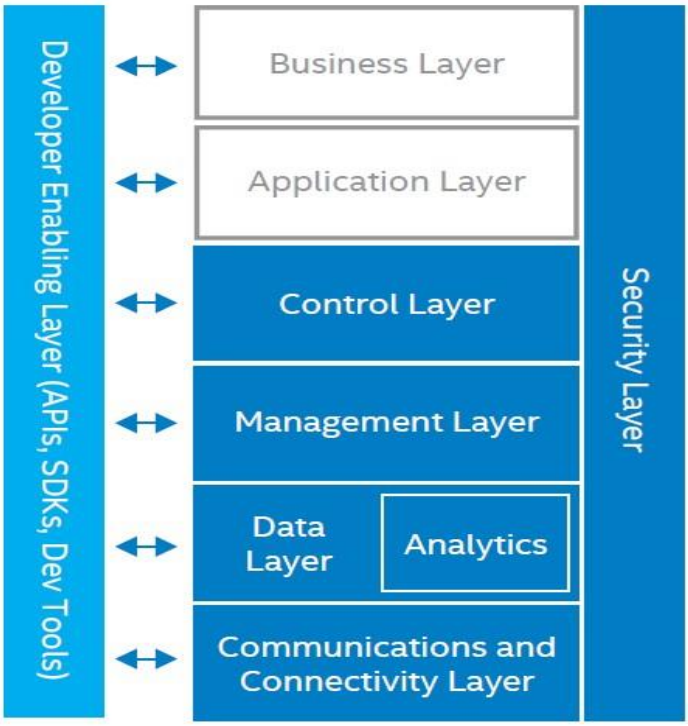


Fig. 10 The Intel IoT platform's architecture (the white blocks represent user layers, the light blue block is the layer for developers, and the horizontal dark blue layers are major runtime layers). Source: [23].

The business layer uses the application layer to access other layers. The details of the functioning of the Intel platform layers and their implementation are given in [23]. The software components that connect devices without native internet connectivity are distinguished in (Fig. 11):

- *On premise components* which are located on end-point devices and gateways.
- *Cloud components* which are responsible for data ingestion from the end-point device, data storage, data analysis, service, scheduling, and security management).

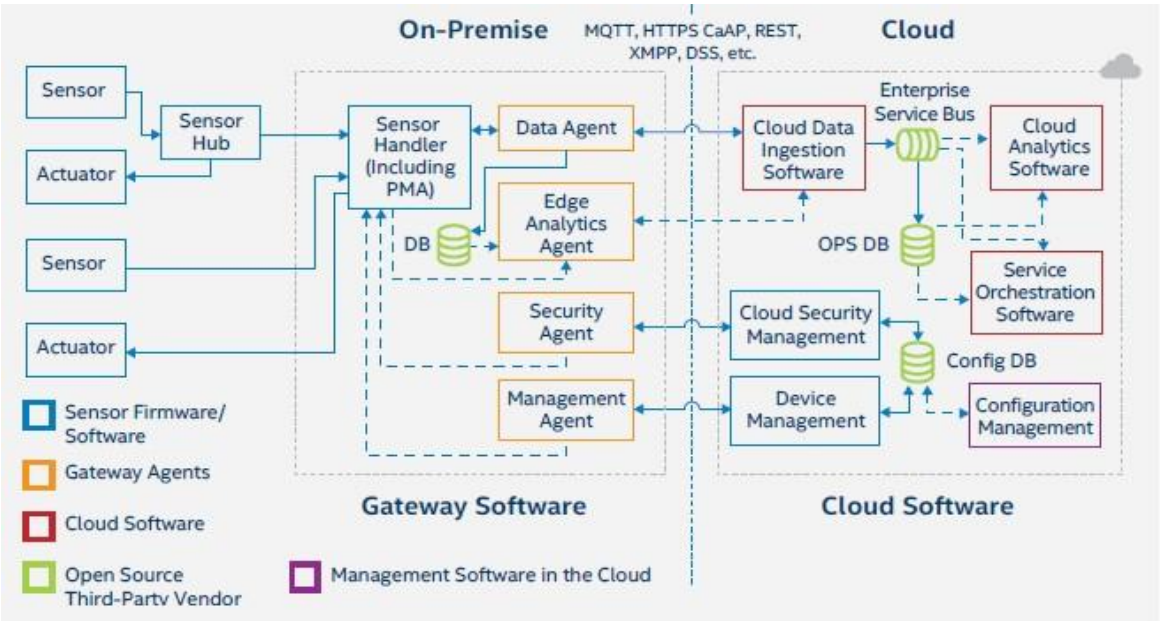


Fig. 11 Software components and interfaces for Intel's IoT reference platform. Source: [23].

The details of the functioning of the Intel platform layers and their implementation are given in [23].
The Intel platform was exploited by Fujitsu in an industrial production fault detection/identification application. Fujitsu used its sensor technology and distributed service platform along with Intel's IoT Gateway aiming at showing how the IoT can provide considerable/measurable value to industrial applications (Fig. 12)

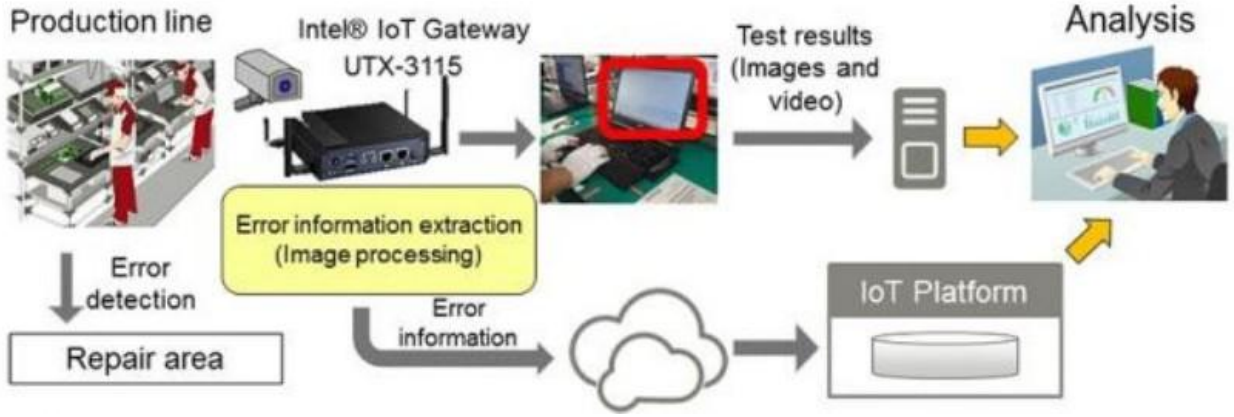


Fig. 12 Fujitsu IoT fault detection system based on Intel's IoT Gateway and Intel's IoT platform.
Source: www.fujitsu.com/global/about/resources/news/press-releases/2016/0519-01.html

The Fujitsu factory was a laptop PCs production line, and with the aid of this fault detection IoT-based system, sought to reduce cost. The analysis of error reports helped the company to identify the misdetection of faults, which allowed the reduction of the incidence of rework. The capability to prioritize rework in real-time led to a 30%reduction of shipping costs by minimizing missed deadlines.

Examples of IoT Applications

IoT finds extensive applications ranging from smart homes to wearables to industrial automation to pollution control to energy management. Overall, IoT enhances the comforts of our lives and provides us more flexibility and controls via the simplification of routine and personal tasks. A partial list of IoT applications is the following: smart homes, smart wearables, smart cities, smart offices, smart agriculture, smart healthcare, smart robotics, smart industrial automation, smart automotive/transportation, smart energy management, smart retail and logistics, smart business [24-29].

Smart homes: A smart home is defined to be one in which the devices can communicate with each other and with their environment. In a smart home one can customize and control the home environment for more security and increased efficiency in energy management. There is a large variety of technologies that can be used for creating smart homes (e.g., smart home lighting, air quality sensing, learning thermostat, smart refrigerator control, etc.) (Fig.13).

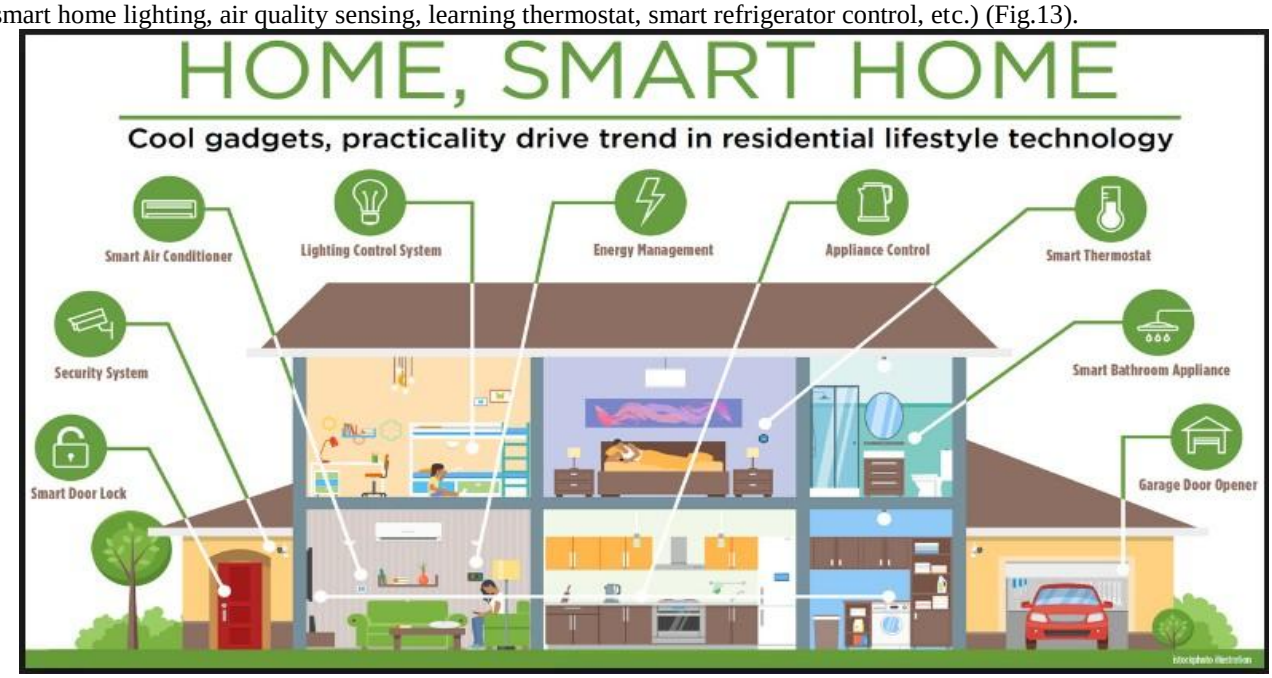


Fig. 13 Smart home IoT components and functions.
Source: https://www.bluebonnetelectric.coop/Community/News/articles/2016/Magazine-Stories/HOME,-SMART-HOME-Trends-in-residential-technology

Smart wearables: Wearable IoT technology is a large field that involves a variety of devices such as health, assistive, and entertainment equipment. Currently, wearables represent one of the hottest trends in IoT use. Examples of smart wearables are:

1. Activity trackers, 2. Smart watches/fitness bands/rings, 3. Smart phones, 4. Interactive socks/shoes, 5. Smart clothing, 6. Smart glasses, 7. Helmets, 8. Headphones/earbuds, 9. Smart jewelry/collars

Some examples of wearables are depicted in Fig. 14.

Fig. 14 A sample of smart wearables.

Source: https://hotline.ccsinsight.com/article/Innovation_in_Smart_Wearables_Flourishes_But_Challenges_Remain

Smart cities: These cities are urban areas that use various kinds of sensors to get and supply data and information for efficient management of community assets and resources. Examples of smart city IoT applications include smart surveillance, smart management systems, automated and safe transportation, environmental monitoring, energy distribution, water network management, monitoring of parking spaces availability, monitoring of material conditions and vibrations in buildings and bridges. Other important applications include monitoring of vehicles and pedestrian levels, adaptive lighting in streets according to weather conditions, measurement of waste container levels, and trash collection. Overall, smart city involves six major components, namely [48]:

- *Smart environment* (green energy, green urban planning, green buildings).
- *Smart economy* (innovation, entrepreneurship, productivity, interconnectedness).
- *Smart people* (inclusive society, digital era education, embrace creativity).
- *Smart mobility* (mixed modal access, integrated ICT, clean and non-motorized option).
- *Smart living* (culturally happy, healthy, safe).
- *Smart government* (transparency and open data, ICT & e-government, policy that enables supply and demand size).

Figure15(a,b) depicts a typical smart city and shows the main smart city features.

(a) **(b)**

Fig. 15 (a) Pictorial illustration of a typical smart city, (b) Smart city features.

Source: https://www.nextgenges.com/iot-enabling-smart-citieswww.ioti.com/smart-cities/world-s-5-smartest-cities (Singapore, Bacelona, London, San Fracisco, Oslo)

Smart offices: A smart office uses several IoT devices (notepads, printers, smart lighting, etc.) that are connected (they talk each other). Ideally, in a smart office everything from the furniture to the copier are connected through IoT. Smart IoT-based office functions include adjustment of room temperature, checking who is at the doors, locking doors, etc. Smart offices can assure great cost saving, e.g., electricity use saving by switching 'on' electronic equipment when it is really needed, automatically turning 'off' unnecessary machines (printers, etc.) after working hours or during weekend/public holidays, and so on. Smart office lobbies provide seamless visitor registration. Guests have the feeling of taken care immediately without waiting for somebody to help them. Other benefits of smart offices, besides energy saving include reduction of e-waste, proactive maintenance, productivity, and cost effectiveness. Fig. 16ashows the icons of some smart office functions, and Fig. 16b shows howa typical smart office looks like.

(a)

(b)

Fig. 16 (a) Icons of smart office functions, (b) Layout of a typical smart office.
Source: (a) https://www.spacematrix.com/content/how-iot-internet-things-shaping-smart-office-future,
(b) https://chaione.com/blog/putting-the-smart-in-smart-office-2

Smart agriculture: The agricultural sector requires highly scalable technology solutions that can be provided by IoT applications. Here, IoT contributes in several ways, e.g., sensor-based field and resource mapping, monitoring soil moisture, remote crop monitoring, control of microclimate conditions for improving fruit and vegetable production and quality, forecasting snow, ice or wind changes, control of temperature and humidity levels to prevent microbial/fungus contaminants, river water quality analysis and management with regard to its use for drinking, smart logistics and warehousing, etc. Agricultural IoT uses medium bandwidth-range single sensors and wireless sensor networks. Figure 17 illustrates pictorially some IoT-based functions of smart farming.

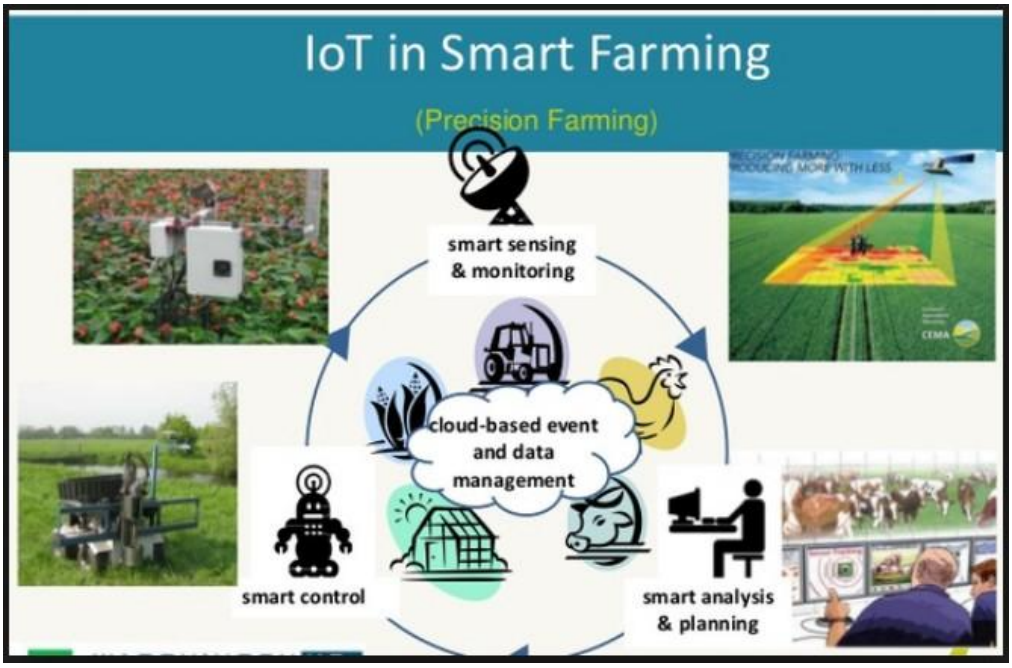


Fig. 17 Smart agriculture/farming IoT-based functions.
Source: https://www.quora.com/Is-there-any-new-method-for-smart-agriculture-using-IOT-tecnology

Smart healthcare: IoTis considerably contributing to medicine and healthcare. The core IoT healthcare applications include automated data gathering, moving objects' tracking, personnel and patients identification, and authentication of people. Object tracking involves patient flow monitoring for improving workflow in hospitals. Identification and authentication involves patient identification for reducing incidents harmful to them, infant identification in hospitals for preventing mismatching, maintenance of medical records, tele-monitoring patient conformance with medication schedule, etc. IoT components used in healthcare include RFID, NFC, WSN, WiFi, Bluetooth, etc. Figure 18 shows a smart home integrated with smart health care functions for the elderly (remote service, wearable sensing, activity detection, sleep monitoring, etc.).

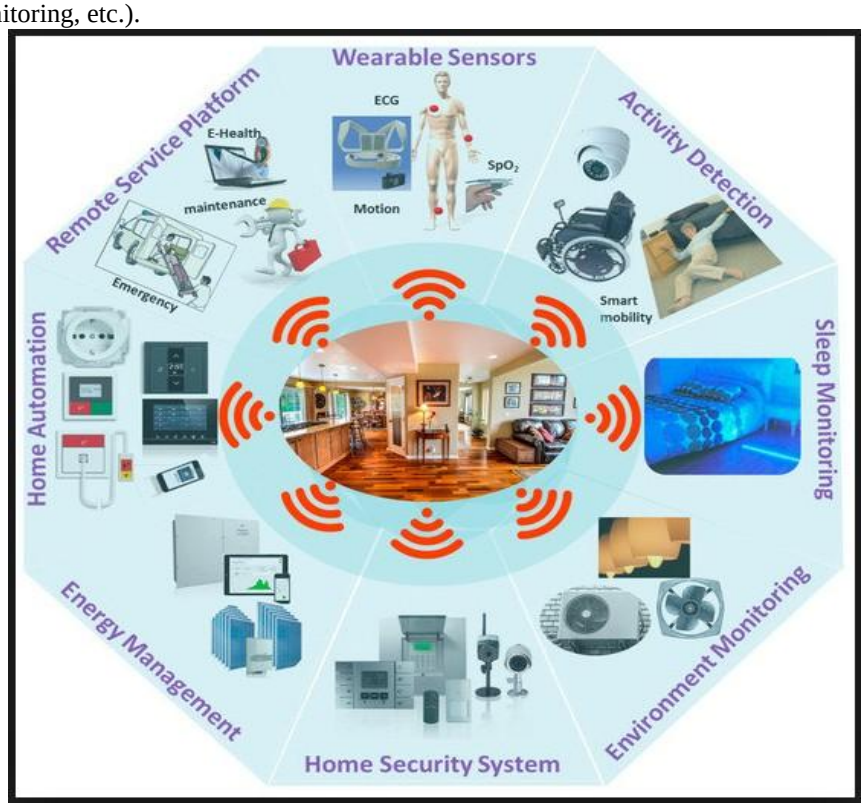


Fig. 18 Smart elderly healthcare integrated in a smart home.
Source: www.mdpi.com/1424-8220/17/11/2496

Smart robotics: The incorporation of robotic issues into the wider IoT was called by ABI Research *"Internet of Robotic Things"* **(IoRT)**. IoRT is actually concerned with *machine to machine* **(M2M)** communication between robots and devices in an ecosystem in where data are leveraged to drive insights and actionable outcomes. The robot is an intelligent device in the sense that it can monitor events and fuse data from several sources in order to determine and execute a best course of action, e.g., a move through the physical environment and manipulation of objects in this environment in a desired way. Potential applications of IoRT include:

- Use a robotic device to check if a car is allowed to use a given park lot in a corporate parking area.
- Collaboration of IoRT and humans in a manufacturing unit to make operational and other decisions.
- Use of IoRT for elderly assistance and domestic cleaning.

Smart industrial automation: This constitutes one of the major application areas of IoT. With the aid of IoT infrastructure, advanced sensor networks, wireless connectivity, and M2M communication, conventional industrial automation is modernized completely. Most industries (small and large) have already adopted and are using IoT enhancements. IoT based industrial automation represents the present state of automation, called industrial automation 4.0 or *"Industrial Automation Internet of Things"*(**IAIoT**). Figure 19a depicts a set of interconnected IoT automation devices, and Fig. 19b a set of IoT devices of general use.

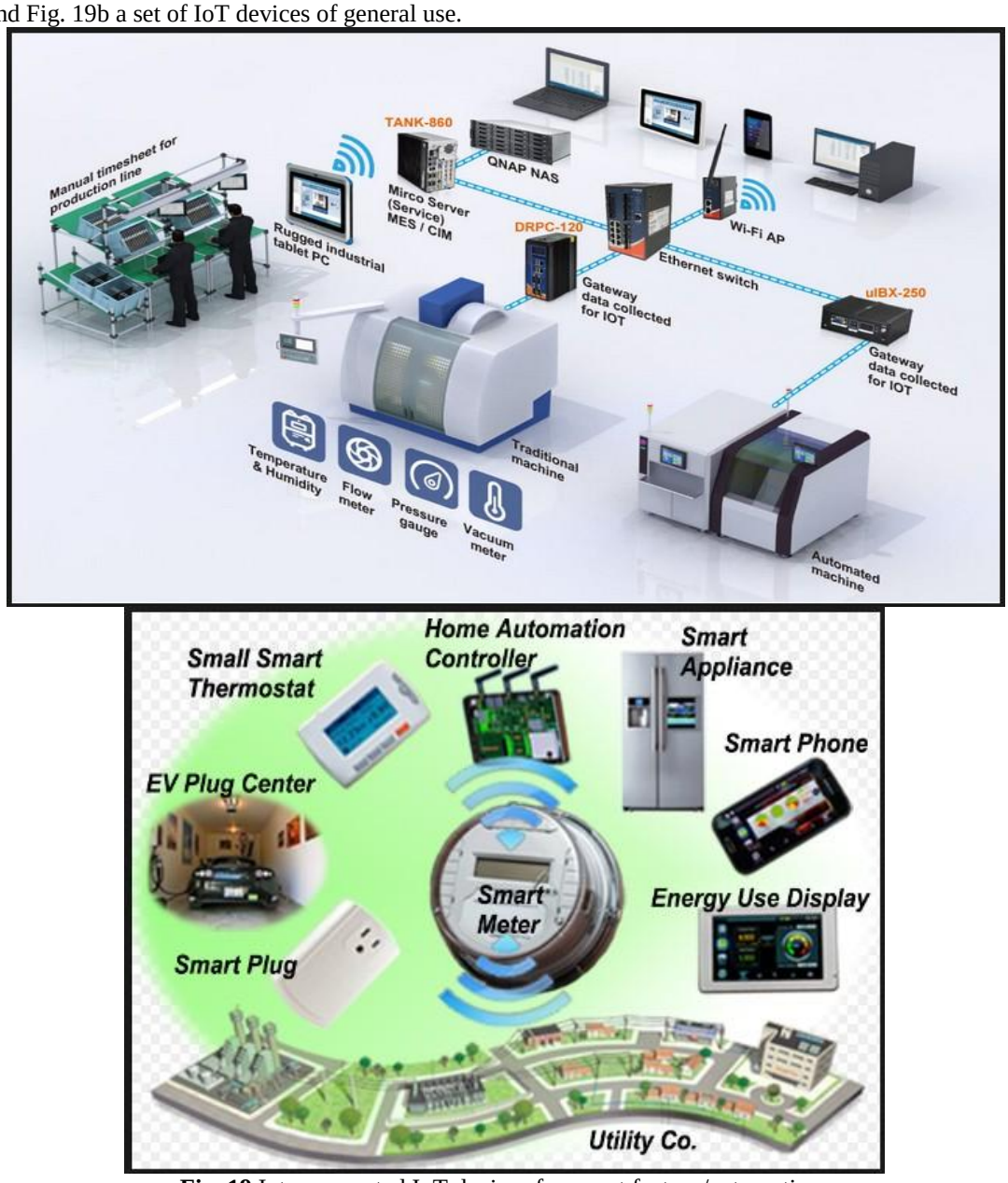


Fig. 19 Interconnected IoT devices for smart factory/automation.
Source: www.fusion4freedom.com (Tom D. Tamarkin)

Smart automotive/transportation: IoT can help to manage transportation and traffic congestion much better than current standard networks. Cars equipped with IoT sensors can monitor traffic and transmit the information to a centralized control system which sends feedback to vehicles on road according to an optimal traffic control law (e.g., regulating the speed limits in congestion areas, suggesting shortest possible routes for reaching desired destinations, etc.). Drivers may also be aware through the car sensor network about school areas where there may be groups of children crossing the roads, and informed about alternative routes to their destinations. Other areas where IoT can help in transportation include: smart transport logistics, smart security and surveillance systems, smart reservation ticketing and toll systems, and end to end (e2e) intelligent transport solutions. A development of connected cars is the so-called "Internet of Cars" (IoC) pictorially illustrated in Fig. 20. Figure 21 shows future opportunities of IoT connected cars.

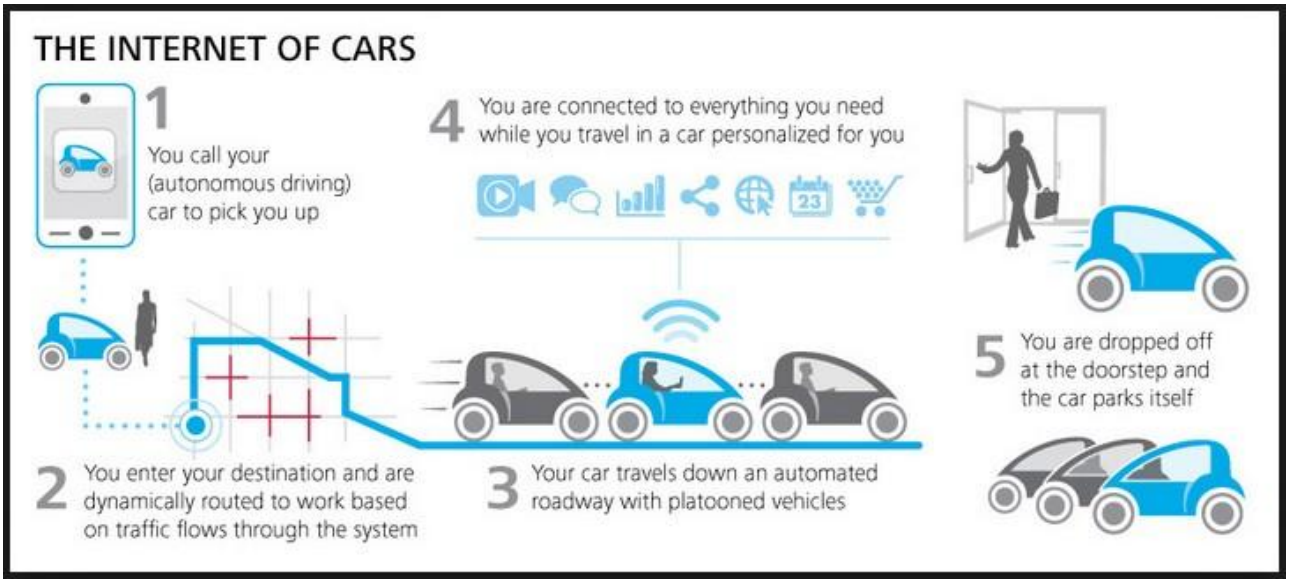


Fig. 20 Pictorial illustration of the Internet of Cars.
Source: www.government-2020.dupress.com/trend/connected-vehicles/ (According to Strategy Analytics, by 2025 more than 50% of cars will be equipped with GPS navigation).

Fig. 21 Smart/IoT connected cars applications/opportunities.
Source: https://internetofbusiness.com/5026-2/

Smart energy management: This area of IoT applications finds increased popularity with the use of power grids that are very smart and highly reliable. Smart grids collect data in an automated way and analyze the behavior of electric energy suppliers and consumers aiming at improving both the efficiency and economics of electricity use. Fig. 22 gives a pictorial view of smart electricity infrastructure which can be fused with advanced technologies, government policy, and consumer input.

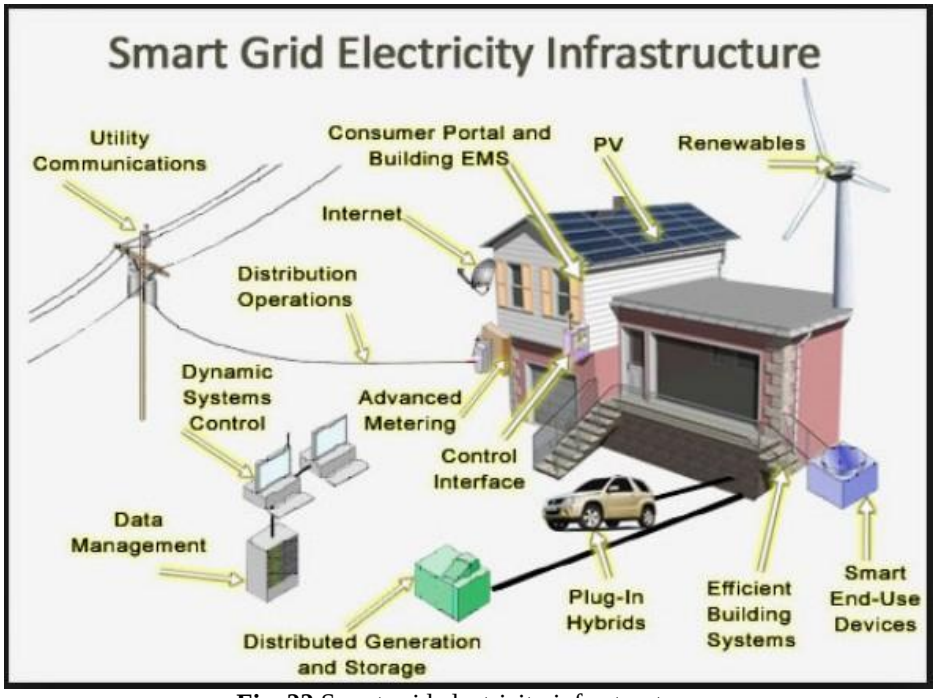


Fig. 22 Smart grid electricity infrastructure
www.smartgrid.ucla.edu, https://mayocommunications.wordpress.com

Smart retail and logistics: IoT finds extensive application in retail and logistics. The proximity-based advertising model of smart retailing is already a reality. We have already IoT application examples in smart supply chains. For example, in chain management IoT contributes in monitoring of storage conditions along the supply chain. IoT can also facilitate product tracking for traceability purposes and payment processing on the basis of the location and duration of various operations (public transport, car parking, etc.).Particularly, IoT can help in guiding customers in a shop according to their shopping list, and in restock processes of products in shelves. Actually, using IoT-based retailers can reduce theft, and increase purchases via cross-selling and more accurate inventory control. Figure 23 shows a number of smart retail functions.

Fig. 23 Smart retail functions
https://umento.sg/smart-retail

Smart business: The adoption of IoT in business improves interest rate, and brings a change in business processes leading to cost minimization and quality improvement. Customers of a product can be easily monitored, and assets following and inventory control are facilitated. In general, IoT business models with smart components for monitoring, control, optimization, and automation are distinguished in two categories:

(ii) Enhancement of available products with IoT add-on services (e.g., refrigerators that order goods autonomously, or dishwater that orders dishwashing tasks by itself).

(i) Development of IoT products that is impossible to exist without IoT (e.g., portable fitness components that collect health-related data such as people's intensity of motion, sleep patterns, etc.).

Figure 24 depicts six IoT devices used in business. Smart (Internet-connected TV) is now found in many lobbies and conference rooms. VOIP Phone is for communication over an IP connection.

Fig. 24 IoT devices for business.
Source: https://www.armis.com/6-iot-devices-compromising-business

IoT Advantages and Disadvantages

IoT offers many advantages, but at the same time has several disadvantages. The principal of them are the following [30-34].

Advantages

- ***Communication and connectedness:*** IoT supports communication between *devices and machines* (M2M communication) and between *humans and machines* (H2M communication) enabling them to stay connected, and so making total transparency available with better quality. For example, in a factory with IoT connected machinery, operational information can be transmitted to partners (suppliers, field engineers, etc.), thereby enabling factory and operational managers to smoothly control the factory units so as to exploit advantageously process optimization and automation.
- ***Monitoring:*** This is one of the major advantages of IoT. For example, knowing the precise quantity of supplies or the air temperature level of a home can give more information that could not be otherwise collected.
- ***Impact to society:*** IoT benefits all (individuals, community, business stakeholders), and, in general, through lower energy consumption and faster delivery of services, etc., contributes to the betterment of society and people's quality of life.
- ***Money saving:*** This is the biggest benefit of IoT for both individuals and companies or enterprises. Through efficient interconnection and sharing of devices, our work, our services and our systems are made cheaper and more efficient.
- ***Accuracy:*** IoT involves a huge amount of data. Analyzing large amounts of data allows one to make right decisions easily and perform tasks accurately. The more the data analyzed the more accurate the decisions made. In general, the more information and the more knowledge, the better. For example, having more information helps us to know what to buy at the supermarket or if our enterprise has sufficient stocks and supplies.
- ***Time:*** Time means money. IoT helps to save a lot of time. In present days, all of us need more valuable time. For example, IoT helps us not to repeat the same tasks every day, and thus enables us to spend our time to other more demanding or creative tasks.
- ***Improved customer engagement:*** In standard information applications, customer engagement is normally passive or very little. In IoT this is completely changed. Customers are actively engaged in the processes and functions involved.

Figure 25 illustrates the two major ways of connectivity.

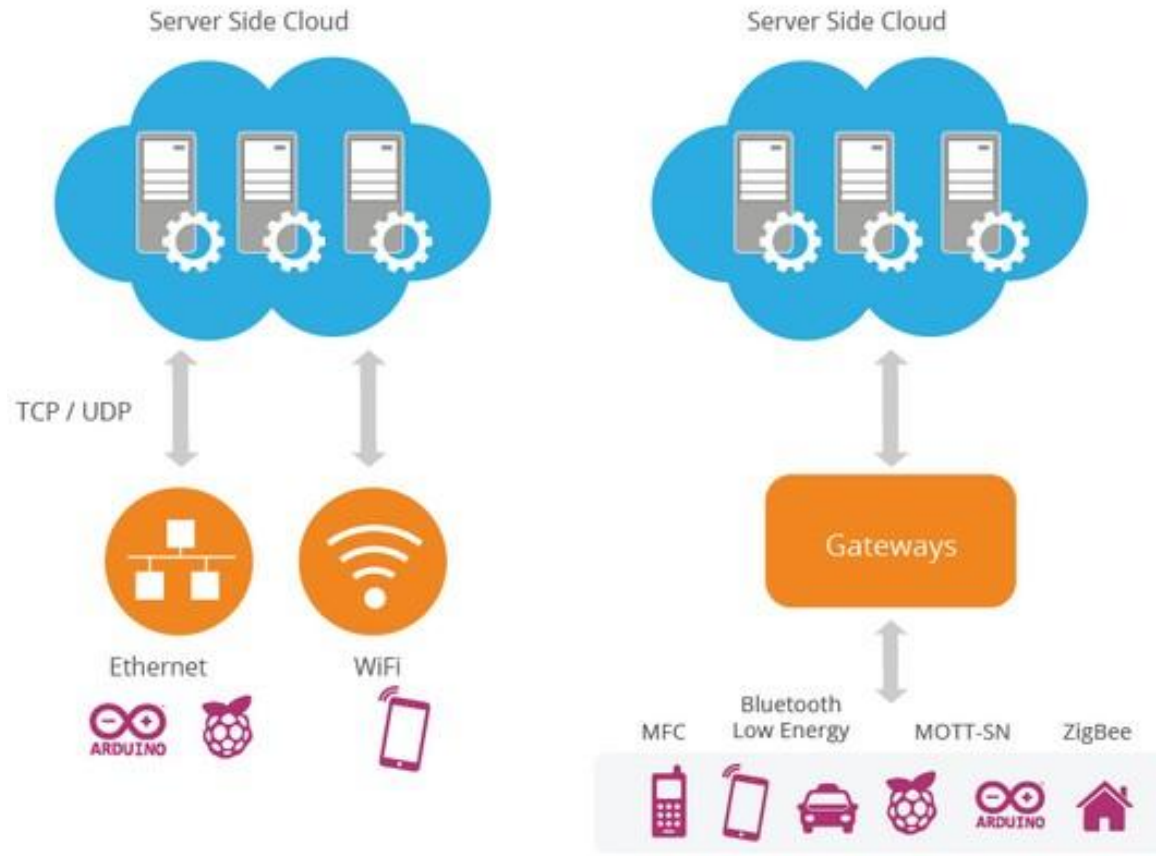


Fig. 25 Major connectivity modes.(a) Through TCP/UDP and Ethernet or WiFi, (b) Through Gateways and MFC/Bluetyoot/MOTT-SN/ZigBee. (Gateway is a key component in many IoT applications, particularly in industrial IoT (IIoT).

Source: https://theexuberantindian.wordpress.com/2017/17/04/16/iot-architecture-reference-model

In gateways, legacy data collection is combined with protocols to present information in an industrial or enterprise system easily and without disruption. This is a fundamental element of deploying IIoT solutions, as contrasted to M2M systems that work independently of each other.

Disadvantages

- ***Privacy and security:*** IoT is supported by multiple technologies and so multiple inventors are involved in it. This creates the danger of privacy threat. IoT is now attracting strong attention by hackers and cybercriminals. In the past, devices from smart phones to smart cars to smart homes to industrial controllers and consumer electronics were of little interest to hackers, but in present days cybersecurity is a crucial issue.For example, an attack to the IoT network can disturb its crucial deployments and as a consequence may expose a risk to the privacy of people. Security algorithms and precautions by users can help avoiding any security related threats and identity theft, because in IoT the details of things are openly available. Such precautions include, but are not limited to, the following:
  1. Passwords should not be stored anywhere in internet cloud. It is advisable to change regularly the password of IoT devices to maximize security.
  2. Third party software should be authentic. Authenticity should be verified.
  3. Unused IoT devices should be switched off because they are vulnerable for potential attack by hackers.
  4. Finance, business, and banking related companies should store the data and retain them only as long as they are needed. They should delete them afterwards to minimize the probability of hacking.

A full discussion of the security and privacy issues in a large set of IoT applications is provided in [33].

- ***Complexity:*** The IoT environment is complex and its design, maintenance and deployment are very difficult. Therefore as with all complex systems there is higher possibility of failure.
  For example, a bug in the software may lead to an automatic order of a new ink cartridge for your printer each and every hour for a few days. An error in the design may cause major faults in its components that

may lead to disasters, e.g., in an IoT-based and automatically operated dam, an erroneous measurement of the water level may cause the gate to wrongly opened, and render a city inundated.

- ***Component compatibility and interoperability:*** There is not IoT interoperability standard, and so interoperability of components from different manufacturers remains a challenge.
  Extensive compatibility and interoperability tests are required before launching an IoT system for use, which implies increased cost on the IoT device manufacturers and the providers of IoT services.
- ***Safety risk:*** Using IoT, safety is ultimately in the hands of the consumer. For example suppose that a hacker changes the medical prescription of a person, or an e- store sends you a product that you are allergic to, or a product that it is already expired. You have always to suspect the product and check it carefully. On the other hand, your safety is at risk if private and confidential/sensitive information is accessed by unauthorized people. A question here is how well encrypted should the data be kept and transmitted?
- ***Compliance:*** The complexity of IoT makes much more difficult the compliance with regulations and legislation. With standard software compliance, the issue of IoT compliance seems to be a very challenging problem.
- ***Societal issues:*** Automating every day activities and using IoT in business and industry, the need for human resources will be naturally reduced, and this may create unemployment in the society. Technology is increasingly embedded and controls our lives. Super reliance on technology (Internet, IoT, automation) and dependence on it, exhibits more chances of potentially harm events if we lose it. Young people are already using technology for every little thing. The question here is how much of our daily activities should we allow to be mechanized and controlled by machines.

IoT Components

Here a number of basic hardware IoT components and software applications are listed.

IoT Hardware

These components include components for a remote dashboard, control devices, servers, sensors, and routing devices. The standard hardware devices, namely the desktop, tablet and cellphone remain integral parts of IoT as the control center and remotes. Other primary connected devices are key network devices (routers, switches, etc.).The desktop enables the user to exert the highest level of control over the system. With the tablet, the user can access the major features of the system in a similar to the desktop way. The tablet also performs as a remote. The cell phone enables the user to do some changes of principal settings, and also provides some functionality. Other IoT hardware components include wearables and sensors [34]:

- ***Wearables:*** These are small electronic devices worn on the head (helmet, glasses), neck (jewellery, collars), arms (watches, wristbands, rings), torso (clothing, backpacks), and feet (socks, shoes).
- ***Sensors:*** These devices constitute the most important IoT hardware devices. A partial list of IoT sensors is the following: acoustic sensors, pressure sensors, humidity sensors, gyroscopes, accelerometers, magnetometers. The functioning of some sensors is as follows [34]:
  -*Accelerometers* detect changes in gravitational acceleration of the device it is mounted on (e.g., smart phone, game controller).
  -*Smart grid sensors* provide real-time data about grid conditions detecting failures and alarms.
  -*Photosensors* detect the existence of visible light and/or ultraviolet energy.
  -*Wireless sensor networks* involve specific sensors/transducers that are placed in a communication infrastructure for monitoring pressure, humidity, temperature, etc., and recording environmental conditions at different locations.
  -*LIDAR:* this is a laser-based method for range finding and mapping that typically uses an eye-safe low-power pulsing laser operating in combination with a camera.
  -*CCD:* Charge-coupled device: this device stores and displays the data for an image, converting each pixel into an electrical charge according to a color in the color spectrum.

The principal categories of IoT hardware components are given in Fig. 26.

IoT Software

IoT software deals with the areas of networking and action. It is functioning through the use of platforms, embedded systems, cooperating system, and middleware. The individual and master software applications perform the following [35]:

- ***Data collection:***Here the following functions are performed: sensing, measurement, data filtering, data aggregation, data distribution, and data security. Finally, the data are sent to a central server.
- ***Device integration:*** This software integrates (binds) the system components to make the core of the IoT system.
- ***Real time analysis:***This software gets data, signals or inputs from several IoT devices and provides viable actions or patterns for human analysis, to provide data required by industry or automation systems. A stable communication and cooperation between multiple devices must be assured.

- ***Application and process extension:*** These software applications enable the IoT system to integrate specific devices for desired purposes (e.g., allow certain mobile devices and other instruments access). They also help to collect data more accurately and get increased productivity.

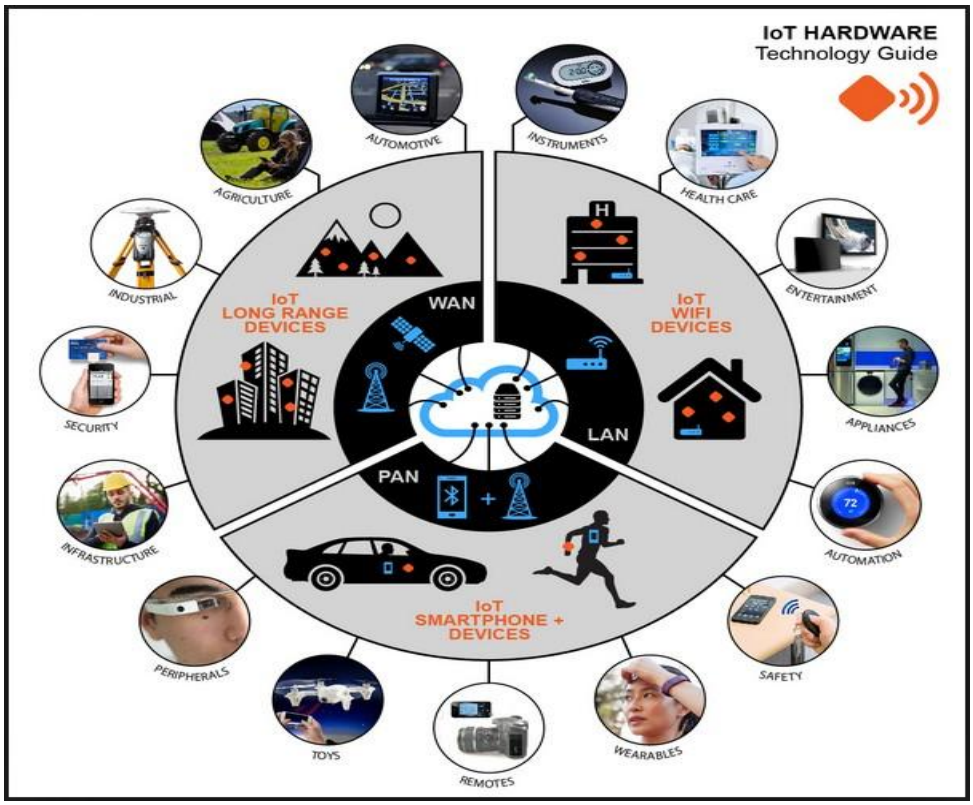


Fig. 26 A wide repertory of IoT hardware devices (IoT Hardware Technology Guide).
Source: https://www.rooksecurity.com/building-security-into-iot-development/iot-device-category-guide

Conclusions

This article provided a holistic conceptual tour to the Internet of Things (IoT) covering IoT definitions, IoT characteristics, IoT architectures and platforms, IoT applications, IoT components (hardware, software), and IoT advantages and disadvantages. IoT is actually the next stage of the Internet in which things/objects with sensors and actuators are connected in the Internet such as they can get data and lead to smarter relations, including in some cases specific actions upon data. A comprehensive literature review of IoT can be found in [36].

It is almost globally estimated that IoT is going to be a very large market, both in terms of device numbers and revenues [37] (Fig. 27).

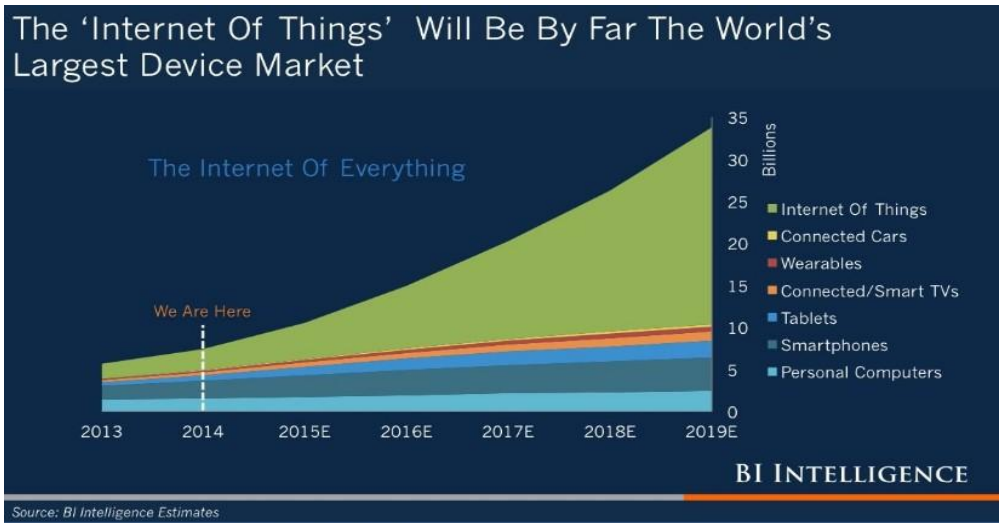


Fig. 27 Distribution of the market of Internet of Everything. The IoT market is estimated to be the World's largest device market. Source: BI Intelligence [37].

Further, according to UK Business Insider [38], the enterprise IoT is predicted to be the largest of the three main IoT sectors, viz.: enterprise, home, and government. It is estimated that there will be a total of 23.3 billion IoT devices, connected by 2019 across all three sectors, with the enterprise IoT being the 40% of the total, i.e., 9.1 billion devices making it the largest of the three IoT services.

Challenging specific topics for further consideration include the following: security and protection of personal data in the cloud computing, people centric (participatory) sensing, data analytics, and encryption. General topics include IoT architectures and platforms, new protocols, standardization, efficiency, and quality of service (QoS). New protocols for sensing in IoT will play a primary role in complete realizations. Participatory sensing will reduce the cost of sensing in the user's local environment. Currently, many European and international initiatives are in the air (including EU-funded R&D Projects), and many others are predicted to emerge across the academia and industry which will allow a coordinated exploitation and implementation of IoT worldwide.

For the convenience of the reader who wants to study deeply the IoT, we mention here a number of important well-written books on IoT that all together cover the entire spectrum of concepts, design issues, and practical applications/uses of IoT, including evaluation issues and prospects for the future. These books are listed in [39-47].

REFERENCES

[1]. K.K. Patel and S.M. Patel, Internet of Things-IoT: Definition, characteristics, architecture, enabling technologies, applications, and future challenges. *International J. of Engineering Science and Computing*, 6(5), 2016, 6122-6131.

[2]. L. Atzori, A. Iera and G. Morabito, The internet of things: A survey. *Computer Networks*, 54, 2010, 2787-2805.

[3]. S. Sarma, D. Brock and K. Aston, The networked physical world. Proposals for engineering the next generation of computing, commerce and automatic identification. *White Paper of the MIT Auto-ID Center*, Cambridge, MA, USA, 2000.

[4]. K. Ashton, That 'Internet of Things' thing. RFID J., 2009. Available at: www.rfidjournal.com/article/print/4986

[5]. ITU: The Internet Executive Summary. *ITU Internet Reports*, 2005. Available at: www.itu.int/osg/static/special-report-the-internetofThings_summary.pdf

[6]. J. Belissent, Getting clever about smart cities: New opportunities require new business models, *Forrester Research*, 2010.

[7]. IEEE: The Institute Special Report-The Internet of Things. Available at: http://theinstitute.ieee.org/static/special-report-the-internet-of-things

[8]. NIST: Global Teams Challenge—Smart America Round Two. Available at: www.nist.gov/cps/sags.cfm

[9]. IETF: The Internet of Things—Concept and Problem Statement, 2010. Available at: http://tool.ietf.org/id/draft-Iee-iot-problem-statement-00.txt

[10]. CASAGRAS Project Final Report: RFID and the inclusive models for IoT. Available at: http://europa/eu/rapid/pressReleasesAction.do?reference=IP/09/740&format=HTML&aged=0&language=EN&guiLanguage-en
www.grifs-project.eu.data/File/CASAGRAS Final Report(2).pdf
www.rfidglobal.eu/userfiles/documents/CASAGRAS26022009.pdf

[11]. D. Miessler, HP Security and the Internet of Things. Available at: http://h30499.www3.hp.com/t5/Fortify-Application-Security/HP-Security-and-The-Internet-of-Things/ba-p/6450208#.U9M6dQsL2s

[12]. IEEE Internet initiative-Internet of Things, Towards a definition of the Internet of Things [Revision 1, 27 May], 2015. Available at: http://iot.ieee.org

[13]. i-SCOOP, The Internet of Things (IoT)—Essential IoT Business Guide (2016-2020). Available at: https://www.i-scoop.eu/internet-of-things-guide/

[14]. J. van den Hoven, Fact sheet-Ethics Subgroup IoT-Version 4.0, *IoT Expert Group, Technical Report*, Delft University of Technology, The Netherlands, 2012.

[15]. N. M. Turab, Internet of Things: a survey of existing architectural models and their security, *International J. of Computer Science and Security*, 17(5), 2017, 197-205.

[16]. P. Sethi and S. Sarangi, Internet of Things: Architectures, protocols, and applications, J. Electrical and Computer Engineering, 2017 (Open Access).

[17]. F. Bonomi, R. Milto, P. Natarajan and J. Zhu, Fog computing: A platform for IoT and analytics, In: *Big Data and Internet of Things: A Road Map for Smart Environments*, Berlin, Germany: Springer, 2014, 159-186.

[18]. M. Weyrich and C. Ebert, Reference architectures for the Internet of Things, *IEEE Software*, Jan.-Feb. 2016, 112-116.

[19]. RAMI 4.0: Reference architecture model industrie 4.0, *Status Report, VDI/VDE Society Measurement and Automatic Control*, July 2015.

[20]. P. Fremantle, A reference architecture for the internet of things, WSO2. Available at: https://ws02.com/whitepapers/a-reference-architecture-for-the-internet-of-things/#03

[21]. J. Lee, How to choose the right IoT platform: The ultimate checklist. Available at: https://hackernoon.com/how-to-choose-the-right-iot-platform-the-ultimate-checklist-47b5575d4e20
[22]. O. Nawaz, Adopting an IoT platform: Things to know and pitfalls to avoid' Available at: https://www.altoros.com/blog/adopting-an-iot-platform-things-to-know-and-pitfalls-to-avoid
[23]. Intel White Paper, The Intel IoT platfotm: Architecture Specification white paper internet of things (IoT). Available at: https://www.intel.com/content/www/us/en/internet-of-things/white-papers/iot-platform-reference-architecture-paper.html
[24]. M. Rahul, IoT applications with examples, *Internet of Things Wiki Com.*, Jan. 30, 2016. Available at: https://internetofthingswiki.com/iot-application-examples/541/
[25]. R. Porkodi and V. Bhuvaneswari The Internet of Things (IoT) applications and communication enabling standards: An overview, *Proceedings of International Conference on Intelligent Computing Applications (ICICA)*, Coimbatore, India, 6-7 March, 2014.
[26]. J. Sherly and D. Somasundareswari, Internet of things based smart transportation systems, *International Research J. of Engineering and Technology (IRJET)*, 2(7), October, 2015.
[27]. RedHat, Smart transportation applications in the internet of things. Available at: www.iot-transportation-technology-overview-201608-en-pdf
[28]. 10 Real World Applications of Internet of Things (IoT) explained in videos. Available at: https://www.analyticsvidhya.com/blog/2016/08/10-youtube-videos-explaining-the-real-world-applications-of-internet-of-things-iot/
[29]. Internet of Things applications. Available at: https://mindmajix.com/internet-of-things-applications
[30]. What can be advantages and disadvantages of IoT technology? Available at: https://www.quora.com/What-can-be-advantages-and-disadvantages-of- IoT-Internet-Of-Things-Technology
[31]. Advantages of IoT; Disadvantages of IoT, Internet of Things. Available at: www.rfwireless-world.com
[32]. W. Drew, Internet of Things (IoT): Pros and Cons. Available at::https://www.keyinfo.com (/pros-and-cons- of-the-internet-of-things-iot/), Sept., 2016.
[33]. C. Maple, Security and privacy in the internet of things, *J. of Cybernetics Policy*, 2(2), 2017, 155-184.
[34]. https://internetofthingsagenda.techtarget.com/definition/sensordata
[35]. Internet of things: Quick Guide, Tutorials point-simply easy learning. Available at: https://www.tutorialspoint.com/internet_of_things/internet_of_things_quick_guide.htm
[36]. S. Madakam, R. Ramaswamy and S. Tripathi, Internet of Things (IoT): A literature review, *J. Computer and Communications*, 3, 2015, 164-173. Available at: http://www.scirp.org/journal/jcc
[37]. B. O'Donnell, The IoT opportunity is incredibly diverse and still wide open, Techspot.Com News, May 26, 2015. Available at: https://www.techspot.com/news/60786-iot-opportunity-incredibly-diverse-wide-open.html
[38]. J. Greenough, The corporate 'Internet of Things' will encompass more devices than the smartphone and tablet markets, *Business Insider*, UK, Feb. 25, 2015. Available at: https://uk.business insider.com/the-enterprise-internet-of-things-market-2014-12.
[39]. B. Sinclair, How Your Company Can Use Internet of Things to Win in the Outcome Economy,*IoT Inc.*, 2017. Available at: https://www.iot-inc.com
[40]. A. Gilchrist, Internet of Things security issues, Berlin, Germany: *Walter de Gruyter Publishing* House, Jan. 2017.
[41]. P. Waher, Learning Internet of Things, Birmingham, UK: *Packt Publishing*, 2015.
[42]. M. Hung (ed.), Leading the IoT: Gardner Insights on How to Lead in a Connected World, *Gardner, Inc.*, 2017.
[43]. M. Kranz, Building the Internet of Things: Implement New Business Model Disrupt Competitors, Transform Your Industry, New York, USA: *Wiley*, 2016.
[44]. A.C. Raman and P. Raj, The Internet of Things: Enabling Technologies, Platforms, and Use Cases, Boca Raton, USA: *CRC Press*, 2017.
[45]. R. Buyya and A.K. Dastjerdi (eds.), Internet of Things: Principles and Paradigms, Cambridge, MA, USA: *Morgan Kaufmann (Elsevier)*, 2016.
[46]. F. da Costa, Rethinking the Internet of Things: A Scalable Approach to Connecting Everything, *A press Open*, 2013.
[47]. J. Rossman, The Amazon Way on IoT: 10 Principles for Every Leader from the World's Leading Internet of Things Strategies, Vol. 2, *Publisher John E. Rossman*, Oct. 2016.
[48]. https://smartcity.org.hk/index.php/aboutus/background