Chapter 9. IoT - The advanced level of the Internet

Table of Contents

The Internet of Things (IoT) is the network of physical objects accessed through the internet as described by technology analysts and visionaries. These objects contain embedded technology to interact with internal states or the external environment. That is, when objects can sense and communicate, it changes how and where decisions are made, and who makes them. The Internet of Things can be seen as scenario in which objects, animals or people are provided with unique identifiers and the ability to automatically transfer data over a network without requiring human-to-human or human-to-computer interaction. This is a term that we are hearing nowadays, and will be hearing in the future as well.

Internet of Things can be identified as a network which has uniquely identified and communicating objects with a certain protocol. From an other aspect, we can say a system with a smart network which is consisted by communicating devices.

Internet of Things has evolved from the convergence of wireless technologies, micro- electromechanical systems and the Internet. In 1991 at Cambridge University, (nearly) 15 academics found a system which captures the coffee machine. Considering that days, this might be a freaky system because this system was sending 3 photos in a minute to all these academics' computers. Because its an online and real time work, this was the first usage of Internet of things in the history.

Connecting things to the Internet can be accomplished with the help of various protocols and standards, either adopted from the traditional Internet and telecommunications fields (WiFi and Bluetooth, Ethernet, 3G and LTE, HTTP), or specifically tailored to meet the constraints of the connected things (ZigBee and Z-Wave, as well as IETF's 6LoWPAN, RPL, and CoAP).

What is a Thing?

According to the IoT Clusterbook SRA (Sundmaeker et al. 2010), a "thing" in the Internet-of- Things can be defined as a physical or virtual entity that exists in space and time and is capable of being identified. A thing in the Internet of Things, can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built in sensors to alert the driver when tire pressure is low or any other natural or man-made object that can be assigned a unique identifier and provided with the ability to transfer data over a network.

An IoT object shall have both processing and communication capabilities, either embedded in itself or offered by an attached component . Depending on their functionality, these things generate, relay and/or absorb data. Based on their primary functionality, the IoT objects can be divided into the following three categories (ITU 2005):

- Identifying things assign a (unique) identity to an object.
- Sensing things transduce the physical state of the object and/or its environment into the (digital or analog) signal for storage and further processing.
- Embedded-systems things have an immediate access to the data sensed and processed by the systems.

Naturally, the categorization is non-exclusive; for example, sensors may have identities and embedded systems may include both identifiers and sensors. Different taxonomies are available for classifying the things in IoT; The following table summarizes the dimensions found in literature to characterize or classify the IoT things (Smith et al. 2009; Chaouchi 2010; OECD 2012).

Dimension	Characteristics
Mobility	Moveable vs. fixed
Size	From tiny microchips to large vessels
Complexity	Dumb vs. smart
Dispersion	Concentrated vs. dispersed
Power supply	Externally powered vs. autonomous
Placement	Attached vs. embedded
Connectivity patterns	Sporadic vs. continuous communication, narrow vs. broadband
Animateness	Non-animate vs. animate

Currently, according to actual research, today there is 10-11 billion devices connected to the Internet and it is expected to be 50 billion in 2020. According to the same research, in 2003 there was 0,08 communicating devices for each person, in 2020 its assumed to be 6,48. İn addition, in 2020, its assumed that 20 classical home type devices will create data transfer traffic, which is greater then 2008's all internet data transfers traffic at all.

Definitions

A number of definitions have been provided for the term Internet-of-Things in recent literature.

Note

Original Definition

Bill Joy had envisioned D2D (Device to Device) communication, as part of his "Six Webs" framework (as far back as 1999 at the World Economic Forum at Davos); it wasn't until Kevin Ashton that industry got a second look at the Internet of Things.

In a seminal 2009 article for the RFID Journal, "That 'Internet of Things' Thing", Ashton made the following assessment:

> Today computers—and, therefore, the Internet—are almost wholly dependent on human beings for information. Nearly all of the roughly 50 petabytes (a petabyte is 1,024 terabytes) of data available on the Internet were first captured and created by human beings—by typing, pressing a record button, taking a digital picture, or scanning a bar code. Conventional diagrams of the Internet ... leave out the most numerous and important routers of all - people. The problem is, people have limited time, attention and accuracy—all of which means they are not very good at capturing data about things in the real world. And that's a big deal. We're physical, and so is our environment ... You can't eat bits, burn them to stay warm or put them in your gas tank. Ideas and information are important, but things matter much more. Yet today's information technology is so dependent on data originated by people that our computers know more about ideas than things. If we had computers that knew everything there was to know about things—using data they gathered without any help from us—we would be able to track and count everything, and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling, and whether they were fresh or past their best. The Internet of Things has the potential to change the world, just as the Internet did. Maybe even more so.

—Kevin Ashton, 'That 'Internet of Things' Thing', RFID Journal, July 22, 2009

As of 2014, research into the Internet of Things is still in its infancy. In consequence, we lack standard definitions for Internet of Things. With the potential for great mischief through hacking, security issues are pivotal to the success of systems-integration designs. A survey lists several IoT definitions as formulated by different researchers.

Kevin Ashton (born 1968) is a British technology pioneer who co-founded the Auto-ID Center at the Massachusetts Institute of Technology (MIT), which created a global standard system for RFID and other sensors.

In general, the following three complementary – and partly overlapping – visions can be distinguished (Atzori et al. 2010, Bandyopadhyay and Sen 2011):

1. The Things oriented vision focuses on the things' identity and functionality, which is in line with the original idea which was initially tied to the RFID and Electronic Product Code (EPC), other identification alternatives have emerged, and the concept of an identifiable object has been expanded to include also virtual entities. From this perspective, IoT is defined as:

   > Things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts.

   or

   > A world-wide network of interconnected objects uniquely addressable, based on standard communication protocols. (EPoSS 2008)

2. The Internet oriented vision emphasizes the role of the network infrastructure and is concerned with the applicability of the available (and future) Internet infrastructure, including IP protocol stack and

Web standards for the purpose of interconnecting smart objects. This perspective is promoted by, for example, the IPSO (IP for Smart Objects) Alliance 1 , Internet architecture (Gershenfeld et al. 2004), and Web of Things community, suggesting that IoT shall be built upon the Internet architecture, by adopting and, when necessary, simplifying the existing protocols and standards. From this perspective, IoT can be defined (following the definition by CASAGRAS project) as:

> 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. It will offer specific object-identification, sensor and connection capability as the basis for the development of independent cooperative services and applications. These will be characterised by a high degree of autonomous data capture, event transfer, network connectivity and interoperability.

3. The Semantics oriented vision focuses on systematic approaches towards representing, organizing and storing, searching and exchanging the things-generated information, by means of semantic technologies (Toma et al. 2009; Barnaghi et al. 2012). According to this vision, the application of semantic technologies to IoT

> promotes interoperability among IoT resources, information models, data providers and consumers, and facilitates effective data access and integration, resource discovery, semantic reasoning, and knowledge extraction” [through] “efficient methods and solutions that can structure, annotate, share and make sense of the IoT data and facilitate transforming it to actionable knowledge and intelligence in different application domains. (Barnaghi et al. 2012)

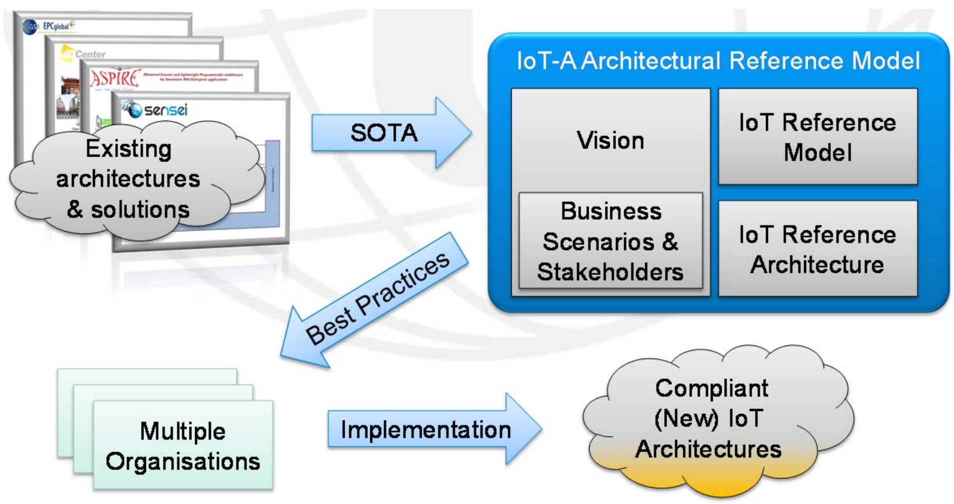
IoT research has its roots in several domains addressing different IoT aspects and challenges. These research domains include, for example, the radio-frequency identification (RFID), machine-to-machine (M2M) communication and machine-type communication (MTC), wireless sensor and actuator networks (WSAN), ubiquitous computing, and web-of-things (WoT). Furthermore, these technologies have been applied in many vertical application domains, ranging from automotive and machinery to home automation and consumer electronics. Thus, what is today known as IoT represents a convergence of multiple domains, and IoT can be seen as an umbrella term uniting the related visions and underlying technologies (Atzori et al. 2010).

The Architectural Reference Model

New applications can only reach its pinnacle if full collaboration between the previously mentioned vertical domains can be achieved. If we consider also the mentioned fact that IoT related technologies come with a high level of heterogeneity (specific protocols, specific applications) in mind, it is no surprise that the IoT landscape nowadays appears as highly fragmented as the following figure shows:

The IOT-A Tree (source iot-a.eu)

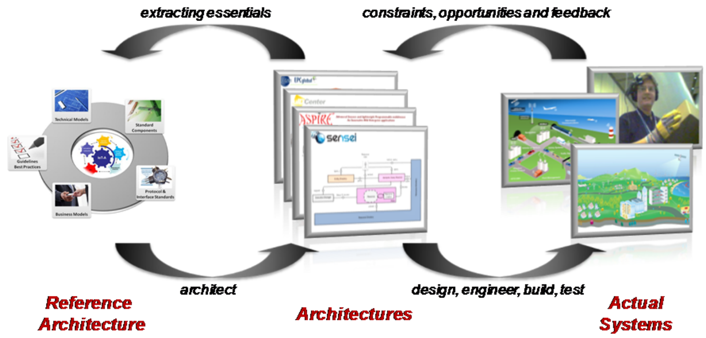
The vision of the Internet of Things IoT-A (http://www.iot-a.eu/arm) wants to promote, a high level of interoperability needs to be reached at the communication level as well as at the service and the information level, going across different platforms, but established on a common grounding. Based on this document, the following figure gives an overview about the building blocks:



IoT-A architectural reference model building blocks (source iot-a.eu)

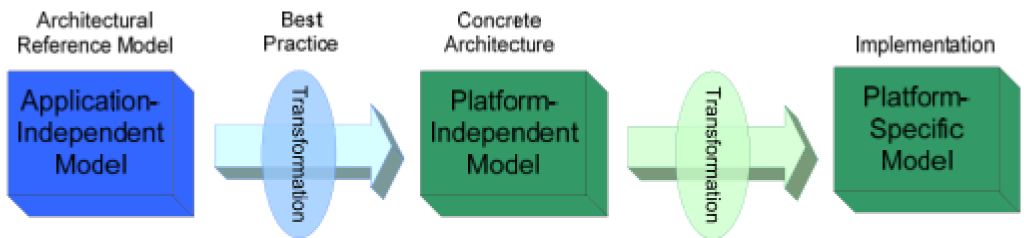
The IoT Reference Model provides the highest abstraction level for the definition of the IoT-A Architectural Reference Model. It promotes a common understanding of the IoT domain. The description of the IoT Reference Model includes a general discourse on the IoT domain, an IoT Domain Model as a top-level description, an IoT Information Model explaining how IoT knowledge is going to be modelled, and an IoT Communication Model in order to understand specifics about communication between many heterogeneous IoT devices and the Internet as a whole. The foundation of the Reference Model is the Domain Model that introduces the main concepts of the Internet of Things and the relations between these concepts. From this model, an other model is derived which holds the structure of all the data that is handled by an IoT system on a conceptual level. The third layer in this vision is the Functional model which groups of functionalities around the key concepts in the Domain model.

The IoT Reference Architecture is the reference for building compliant IoT architectures. As such, it provides views and perspectives on different architectural aspects that are of concern to stakeholders of the IoT.



Relationship between a reference architecture, architectures, and actual systems (adapted from Mueller).

Guidance in form of best practices can be associated to a reference architecture in order to derive use-case-specific architectures from the reference architecture. The role of the ARM is to guide the architect through design choices at hand, and to provide best practices and design patterns for those different choices. It can be visualized as an OMG process for MDA:



Relation of the Best-Practice-driven derivation of concrete architectures from an architectural reference model and the derivation of implementations from said concrete architecture. (source iot-a.eu)

Prev Up Next
Part IV. Internet of Things Home IoT Application