

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/323525875>

Internet of Things (IoT) System Architecture and Technologies, White Paper.

Research · March 2018

DOI: 10.13140/RG.2.2.17046.19521

CITATIONS

6

READS

20,365

1 author:



Ahmed El Hakim

Orange Egypt

2 PUBLICATIONS 8 CITATIONS

SEE PROFILE

Internet of Things (IoT) System Architecture and Technologies

Ahmed El Hakim

Orange Expert – Network Operations

ahmed.elhakim@orange.com

Orange/MEA/MENA/EGYPT/TECHNOLOGY

/CORE AND TRANSPORTS - CONVERGENT NETWORKS

Abstract— the concept of Internet of Things is not new; Devices have been exchanging data automatically in real time without human intervention for years. The IoT is the ability to transform ordinary products such as cars, buildings, and machines into smart, connected objects that can communicate with people, applications and each other. Knowing how to connect machines and equipment, enterprises can generate valuable data, securely transmit these data across multiple networks, collect, store and analyze them in order to turn them into useful information in real time.

This paper presents a theoretical model of Internet of Things (IoT) eco-system architecture and technologies.

I. INTRODUCTION

We live in a world where there is so much to do but so little time. The multitasking capabilities of the present generation is at the highest ever rate. The market is flooded with Technology and Innovations. Yet something seems amiss, that something is “Control”. Control over every Hardware, Electronics, Machine or Technology you own personally as well as professionally. The ability to start stop, monitor, and control and analyse system is what makes the world truly connected. Expanding control over things has been a major intent for humans ever since the advent of fire. The human breed has been ideating to invent and disrupt different sectors to makes life easier and smoother.

Connecting was another important aspect. From discovering new lands across the seas to connecting the people through the internet, the world has come a long way. But do we stop here? Off course not, we see the world as a hyper connected cluster of not only humans, but humans to objects and objects to objects themselves.

This is achieved by IoT. A world which is more connected a world which is smarter. The possibilities are endless, on what we can do and what we can achieve.

In 2008, 'things' connected to the internet were already more in number than people and by 2020 these internet connected things will have already reached 50 billion.[1]

In this paper we provide a theoretical reference model that can be used by operators and network designers to determine the proper setup for IoT inter-communication, system architecture and common technologies.

II. RELATED WORK

With the potential of IoT, there have already been a number of studies addressing aspects of modeling and system setup and technologies of IoT.

Mattern et al. [2] explained that the Internet of Things represents a vision in which the Internet extends into the real world embracing everyday objects. Physical items are no longer disconnected from the virtual world, but can be controlled remotely and can act as physical access points to Internet services. An Internet of Things makes computing truly ubiquitous. Hammersmith Group [3] describes The Internet of Things which comprises a digital overlay of information over the physical world. Objects and locations become part of the Internet of Things in two ways. Information may become associated with a specific location. Alternatively, embedding sensors and transmitters into objects enables them to be addressed by Internet protocols, and to sense and react to their environments, as well as communicate with users or with other objects. Chui et al. [4] explained that the physical world itself is becoming a type of information system. In what's called the Internet of Things, sensors and actuators embedded in physical objects—from roadways to pacemakers—are linked through wired and wireless networks, often using the same Internet Protocol (IP) that connects the Internet. These networks churn out huge volumes of data that flow to computers for analysis. When objects can both sense the environment and communicate, they become tools for understanding complexity and responding to it swiftly. Accenture & Bankinter Foundation of Innovation [5] analyzed that “The Internet of Things (IoT) consists of things that are connected to the Internet, anytime, anywhere. In its most technical sense, it consists of integrating sensors and devices into everyday objects that are connected to the Internet over fixed and wireless networks.

Overall, these studies cover a range of concepts, including ubiquity, unique identification, heterogeneous communication, service, the “smartness” of things and the connection of physical items with the virtual world. In contrast, in our work we aim to define reference model for IoT explaining its ecosystem and used technologies

III. BACKGROUND

In this section, we define the IoT communication and exploring its Eco-system including the function of the key components and elements.

A. Historical Background

The concept of enabling devices with the ability to communicate with each other, without human interaction, has been a subject of experimentation many times throughout the decades. From the 1930s to the 1980s. Radio frequency identification, or RFID, may be a crucial and first technology for IoT. The roots of RFID technology can be traced back to World War II. The Germans, Japanese, Americans and British ,All used radars discovered in 1935 by Scottish physicist Sir Robert Alexander Watson Watt to warn of approaching enemy planes while they were still miles away. But there was no way to identify which planes belonged to the enemy and which were a country's own pilots returning from a mission. The Germans discovered that if pilots rolled their planes as they returned to base, it would change the radio signal reflected back to radar systems. This crude method alerted the radar crew on the ground that these were German planes and not allied aircraft. Essentially, this was the first passive RFID system. Under Watson Watt, who headed a secret project, the British developed the first active "identify friend or foe" (IFF) system. When a British plane received British radar signals, it would broadcast a signal back that identified the aircraft as friendly. RFID works on this same basic concept. A signal is sent to a transponder, which wakes up and either reflects back a signal (passive system) or broadcasts a signal (active system). Advances in radar and radio frequency (RF) communications systems continued through the 1950s and 1960s. Scientists and academics in the United States (U.S.), Europe and Japan explored how RF energy could be used to identify objects remotely. Companies began commercializing anti-theft systems that used radio waves to determine whether an item had been paid for or not. [6]

B. IoT Definition

There are multiple definitions but same concept:

The Internet of things (IoT) is the network of physical devices, vehicles, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to collect and exchange data.[7]

The Internet of Things (IoT) is a system consisting of networks of sensors, actuators, and smart objects whose purpose is to interconnect "all" things, including everyday and industrial objects, in such a way as to make them intelligent, programmable, and more capable of interacting with humans and each other.[8]

The Internet of Things (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. [9]

The scope of IoT is not limited to just connecting things (device, appliances and machines) to the Internet, IoT allows these things to communicate and exchange data (control & information), processing on these data will

provide us various applications towards a common user or machine goal.

* The Global Standards Initiative on Internet of Things (IoT-GSI) concluded its activities in July 2015 to establish the new Study Group 20 on "IoT and its applications including smart cities and communities". All activities ongoing in the IoT-GSI were transferred to the SG20.

C. IoT Ecosystem

The term IoT is used to describe a broad and diverse ecosystem that includes a wide range of different connectivity types and use-cases. Therefore, it is not helpful to discuss the IoT ecosystem as a whole, and to understand IoT better it is necessary to break it down into layers.

The IoT ecosystem has five horizontal layers that are essential elements which is common to all IoT use-cases, regardless of vertical segment as *Figure 1* illustrated [10]:

1. Sensors or controllers (embedded in connected devices, the "things" in the Internet of Things)
2. A gateway device to aggregate and transmit data back and forth via the data network.
3. A communications network to send data.
4. Software for analyzing and translating data.
5. The end application service.

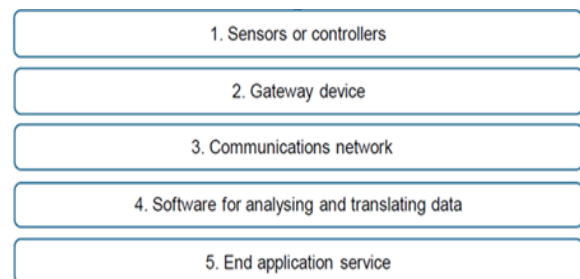


Figure 1. IoT Ecosystem Layers.

That Ecosystem could be considered as a multiple level system with a deeper view of system layers as the multi-level architecture of the IoT World Forum Reference Model which is quite interesting as it illustrates the various levels as *Figure 2* illustrates:[11]

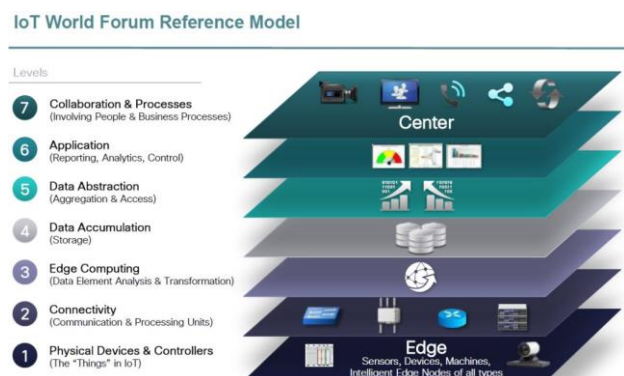


Figure 2. IoT World Forum Reference Model

Physical Devices and Controllers – The model calls this layer the “things” of the internet of things. From a system design perspective, the “things” are the sensors and devices that are directly managed by the IoT architecture.

An important IoT concept, Edge Intelligence, to allow low latency reaction to field events and to allow higher levels of autonomy and distributed processing, needs to be implemented at this layer.

Connectivity – This layer spans from the “middle” of an Edge Node device up through transport to the cloud. Many alternatives can be used for communications and this layer includes the mapping of field data to the logical and physical technologies used as well as the backhaul to the on premise or cloud and the next layer, Edge Computing.

Edge Computing – The next layer in the World Forum Model architecture is Edge Computing, or more properly “Cloud Edge” or “Cloud Gateway” computing. Required to some degree in any IoT system this layer interfaces the data and control plains to the higher layers of cloud or enterprise software layers. Protocol conversion, routing to higher layer software functions and even “fast path” logic for low latency decision making will be implemented at this layer.

Data Accumulation – Given the Velocity, Volume and Variety that IoT systems can provide it is essential to provide incoming data storage for subsequent processing, normalization, integration, and preparation for upstream applications.

Data Abstraction – In the data abstraction layer we “make sense” of the data, collecting “like” information from multiple IoT sensors or measurements, expedite high priority traffic or alarms, and organize incoming data from the data lake into appropriate schema and flows for upstream processing.

Application Layer – This layer is self-explanatory and is where control plane and data plane application logic is executed. Monitoring, process optimization, alarm management, statistical analysis, control logic, logistics, consumer patterns, are just a few examples of IoT applications.

Collaboration and Processes – At this layer, application processing is presented to users, and data processed at lower layers is integrated in to business applications. This layer is about human interaction with all of the layers of the IoT system and where economic value is delivered. The challenge at this layer is to effectively leverage the value of IoT and the layers of infrastructure and services below and leverage this into economic growth, business optimization and/or social good.[12]

Figure 3 and Figure 4 illustrate the IoT system topology and system inter-communications respectively.[13]

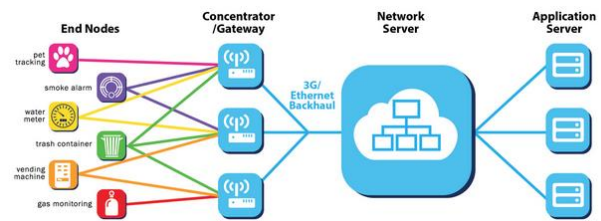


Figure 3. IoT System Topology

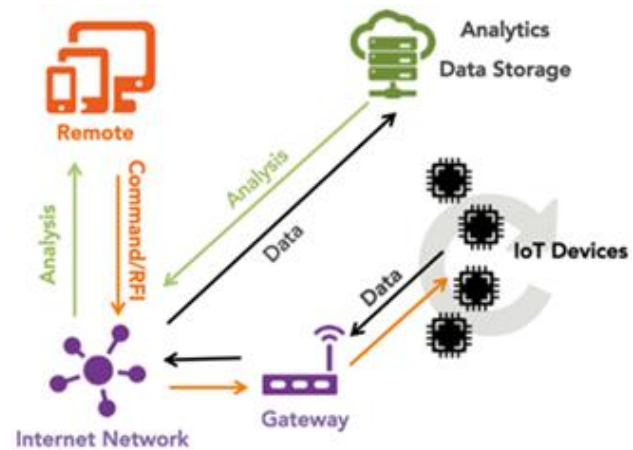


Figure 4. IoT System Inter-communications

IV. IoT TECHNOLOGIES

IoT is not a single technology. It is a combination of sensors, devices, networks, and software that works together to unlock valuable, actionable data from the Internet of Things. Unlike other technologies that revolve around one predominant architecture, device type or connection method, IoT is at its core an assembly of disparate technologies. A connected machine does not become “smart” from a single sensor, or modem, or network, or application alone. It is a combination of all of these pieces coming together that creates added intelligence. There are a range of technologies that enable IoT connectivity, each with benefits and restrictions that are explored below.

The most common connectivity options include Proximity [Like RFID], Wireless Personal Area Networks (WPAN) [Like Bluetooth], Wireless Local Area Networks (WLAN) [Like Wi-Fi], Lower-Power Wide Area Networks (LPWAN) [Like LoRa and SIGFOX] and Cellular or the third Generation Partnership Project (3GPP) standards [Like Second Generation (2G), Third Generation (3G) and Fourth Generation (4G)].

Regarding the unlicensed and licensed frequency bands, the availability of suitable radio frequencies is of great importance for wireless IoT communication. With the exception of cellular, virtually all major technologies are designed for using unlicensed Industrial, Scientific and Medical (ISM) band radio frequencies. The ISM bands are radio frequencies reserved internationally for Radio Frequency (RF) applications for industrial, scientific and medical purposes other than telecommunications.

The worldwide availability of unlicensed radio frequencies is fragmented. 2.4 GHz is the only global ISM-band and used for a wide range of WLAN/WPAN technologies, including Bluetooth and Wi-Fi. Table 1 illustrate the available and reserved unlicensed frequencies for wireless IoT Communication per world region.[14]

Frequency band	Region
169 MHz	Europe
315 MHz	Asia-Pacific
433 MHz	Europe, Middle East & Africa
868 MHz	Europe
915 MHz	Americas, parts of Asia-Pacific
2.4 GHz	Worldwide

Table 1. Unlicensed Radio Frequencies for IoT

Reserved and licensed frequency bands is another option for wireless networking solutions. Some frequency bands, such as 169 MHz in Europe, are reserved for specific industries (in this case utilities). At other times, individual service providers can obtain licensed spectrum for specific applications. As the issue of spectrum re-farming will remain a hot topic for telecom regulators form many years to come, some frequencies may potentially be reserved specific IoT-type applications or specific industries.[14]

A. Cellular

Cellular is a WAN (Wide Area network) with the long-range ability to connect globally using radio waves that are sent and received via cell towers. Strong connections can be made between a device and a cell tower within 16 kilometers. It is also possible to connect to cellular networks via satellite, further eliminating barriers to connectivity in remote areas.[15]

The 3GPP family of cellular networks technologies is the leading platform for wireless communication worldwide. What started out as a single global standard for mobile telephony has evolved into a broad range of 2G, 3G and 4G network technologies that operate across an ever-expanding range of frequency-bands and often supporting multi-mode operation. From our perspective, we divide the 3GPP family of standards into three main categories: the legacy 2G standards like General Packet Radio Services (GPRS), the current 3G/4G High Speed Packet Access (HSPA) , Long-Term Evolution (LTE) and the Emerging 4G-MTC (Machine Type Communication) standards LTE-M and Narrow Band IoT (NB-IoT).

2G [Global System for Mobile (GSM)/GPRS/Enhanced Data Rates for Global Evolution (EDGE) plus Code Division Multiple Access (CDMA)] – is the legacy technology platform used for connecting the vast majority of existing cellular IoT devices. Supporting data rates of up to 50–150 kbps, 2G is sufficient for a wide range of applications. Originally designed to enable voice communi-

cation, 2G technologies are however not fully optimized for data and have limited scalability. 3GPP Release 13 introduced a new feature called Extended Converge-GSM (EC-GSM) that aims to improve the device reachability by up to 20 dB and create a seven-fold improvement in the range of low-rate applications.

3G/4G (HSPA/LTE) – is the leading technology platform for connecting smartphones and other advanced mobile devices. Supporting theoretical peak data rates of more than 100 Mbps, 3G/4G can meet the bandwidth requirements of virtually any IoT use-case. 4G LTE is fully optimized for high-speed data communication with low latency. Top data rates are however achieved at the cost of increased radio complexity and power consumption. To better match the requirements of a wider range of IoT use-cases with low data requirements, LTE CAT-1 was added in 3GPP Release 12, published in December 2014. LTE CAT-1 is optimized for reduced data rates and includes a power saving feature that can support battery life-times of up to 10 years.

4G-MTC (LTE-M/NB-IoT) – is the emerging technology platform for connecting IoT devices to mobile networks. 3GPP Release 13 introduced a number of Machine Type Communication (MTC) enhancements to the LTE standard. The first is referred to as LTE-M (formally eMTC), which defines a new low complexity device category type that supports reduced bandwidth, reduced transmit power, reduced support for downlink transmission modes, ultra-long battery life via power consumption reduction techniques and extended coverage operation. The second is NB-IoT that provides improved indoor coverage, support of massive number of low-throughput Things, low-delay sensitivity, ultra-low device cost, lower device power consumption, and optimized network architecture. 3GPP Release 14 includes improvements for LTE-M and NB-IoT such as multicast and positioning, as well as the new Cellular Vehicle-to-Everything (V2X) for automotive communication.[14]

* The first officially recognized specifications for 5G mobile communications will be included in 3GPP Release 15, which is scheduled for release in the second half of 2018. The 5G New Radio (NR) interface is expected to bring new levels of capability and efficiency, as well as enable new mission-critical control services with low-latency and high reliability communications links.

B. Lower-Power Wide Area Networks (LPWAN)

Lower-power wide area networks are a type of telecommunication network designed to allow long range communications at a low-bit rate for devices such as battery operated sensors. LPWAN work in the license-free ISM frequency bands. Two of the main players in the LPWAN space are LoRa (long range radio) and SigFox. Each have a niche in the market, and warrant a detailed discussion:

1. Long Range Radio (LoRa)

LoRa wide-area network (LoRa WAN) is a LPWAN specification intended for wireless, low-cost, battery operated devices in regional, national or global networks.

LoRa WAN is a product of the LoRa Alliance, an open, non-profit association of industry leaders that believe the IoT era is now, and built the network specifically for IoT/Machine-to-Machine (M2M) connectivity. The goal of the alliance is to standardize LPWANs being deployed around the world to enable IoT, M2M, smart city and industrial applications. The solution is designed to connect over long distances (up to 16 kilometers away), in harsh environments and in isolated areas (e.g., underground). LoRa provides bi-directional communication between end-devices and enterprises via a gateway. This means it is not possible to connect devices as a standalone service, and businesses still require a Wi-Fi or cellular connection to enable communication from the gateway to the server network.[15]

2. SigFox

SigFox is a French company founded in 2009, deploys LPWAN using ISM band frequencies for low-energy objects. The company uses a cellular style system for connecting remote devices, and Ultra Narrow Band (UNB) technology that enables signals to pass through solid objects, making it ideal for devices deployed underground or in rough terrain. In open space the connection range is over 40 kilometers. It also has an extremely reduced power usage rate, making the system practical for remote deployments that cannot be easily accessed for battery maintenance. The standby time for two AA batteries in SigFox connected devices is 10 years or more. However, the network is limited to transmitting only small amounts of data with a wireless throughput of up to 100 bits per second and a payload size of 12 bytes per message.[10] The SigFox network is best suited to M2M use cases that do not require large amounts of data being communicated and/or do not require frequent communication.[15]

C. Wireless Personal Area Networks (WPAN)

Bluetooth is the most famous of WPAN family and considered a short-range connectivity solution. It operates on the license-free, global 2.4 GHz to 2.485 GHz ISM frequency band. It is also able to 'hop' between frequencies to reduce interruptions in connection from other wireless technologies sharing the same ISM spectrum. Due to it being a low bandwidth connection, it is not suitable for transferring large amounts of data; it is best suited to linking sensors and small electronic devices.[15]

Figure 4 illustrates the various characteristic of the IoT main technologies mentioned and common applications compared to each other.





CONNECTIVITY OPTIONS						
		 WLAN	 Bluetooth	 LPWAN		 Cellular
				LoRa	Sigfox	
Characteristics of Options	Frequency Band	Unlicensed, global 2.4 GHz ISM	Unlicensed, global 2.4GHz-2.485GHz ISM	WLAN or Cellular	LPWAN or ISM	Radio frequencies
	Range	Very limited: Maximum 32 meters	Limited: Maximum 100 meters	Good: Max. 16 kilometers	Good: Max 40 kilometers	Very good: WAN (Wide area network) – tower dependent; reliably strong signal up to 16 kilometers from tower
	Unique feature	Ability to transfer large amounts of data quickly	Ability to 'hop' between frequencies	Proven in harsh environments & underground	Very reduced power usage	Long range potential, global connectivity through cell-towers
	Drawbacks	Extremely limited range	Limited range Not suitable to transfer large amounts of data	Can't connect to devices as standalone service	Not suitable to transfer large amounts of data	High power consumption
	Examples	Smart streetlights Parking meters Smart home power meters	Audio & mobile apps Wearables Smart home security sensors	Smart agriculture sensor networks	Remote monitoring systems Alarms	Logistics – asset tracking Transport – keyless locking Smart metering applications

Figure 4. IoT Technologies Characteristic

V. CONCLUSION AND SUMMARY

The Internet of Things is weaving a new worldwide web of interconnected objects.

In this paper, we have presented the IoT technology stack that consists of multiple layers, including device hardware, connectivity, data management, applications and analytics; illustrating a reference model for IoT communication, system architecture and main used wide area networks based on Cellular, WPAN or LPWA technologies.

Finally, The IoT describe the common applications that could be implemented by providers to generate new revenue stream, enhance agility to reach new levels of achievement by accelerating digital business transformation through efficiency, new business and improved customer experience.

VI. REFERENCES

- [1] Demystifying Industrial IoT - White Paper, Winjit.
- [2] "From the Internet of Computers to the Internet of Things" (Mat-tem et al., 2010)
- [3] "The Internet of Things: Networked objects and smart devices" (Hammersmith Group, 2010)
- [4] "The Internet of Things" (Chui et al., 2010/McKinsey & Company)
- [5] "The Internet of Things: In a Connected World of Smart Objects" (Accenture & Bankinter Foundation of Innovation, 2011)
- [6] Towards a definition of the Internet of Things (IoT), Revision 1 May 2015, IEEE.
- [7] Wikipedia.
- [8] IEEE.
- [9] ITU, ITU-T Y.2060 (06/2012).
- [10] The IoT ecosystem, Oct. 2016, STL Partners.
- [11] IoT World Forum, IoTWF 2017
- [12] IoT Architecture, iot-transformation, iot-world-forum, Juxtology.
- [13] BI Intelligence Aug. 29, 2016, Business Insider.
- [14] Cellular and LPWA IoT Device Ecosystems, M 2M Research Series 2017, Berginsight.
- [15] Globalized M2M & IoT Connectivity white paper, Emnify.