International Journal of Computing Academic Research (IJCAR)
ISSN 2305-9184 Volume 4, Number 4 (August 2015), pp.214-223

http://www.meacse.org/ijcar

Improved Layered Architecture for Internet of Things

Dina Gamal Darwish
33 ElRoda Square, ElManial, Cairo, Egypt

Abstract

The internet of things (IoT) is a concept that has a role in facilitating people lives through the use of tablets, smartphones, PCs and other devices connected to the internet. Knowing that the number of people using connected devices on the internet increases every year dramatically. Also, internet of things (IoT) provides a vision of the future internet where connecting physical things; from backnotes to bicycles through a network letting them take an active part in the Internet and exchanging information about themselves and their surroundings, which gives immediate access to information about the physical world, leading to innovative services and increasing efficiency and productivity. This paper proposes an improved architecture to the internet of things (IoT) that takes into consideration the environment surrounding the devices, including the objects to be detected or the places to observed, and other factors affecting the sensing operation. Finally, conclusions are made and future work is discussed briefly.

Keywords: Internet of Things (IoT), Layered Architecture, Network Layer, Hardware Layer, Environment Layer.

Introduction

There are many definitions of the Internet of Things (IOT) that arised nowadays. One of the most known definitions is currently provided by the U.S. National Intelligence Council [1] "The "Internet of Things" is the general idea of things, especially everyday objects, that are readable, recognizable, locatable, addressable, and controllable via the Internet - whether via RFID, wireless LAN, wide-area network, or other means."

An important thing is that while the most common Internet-connected devices are computers such as laptops, servers, smartphones, and tablets (e.g., iPads, *etc.*), the IOT concept is much broader. In particular, everyday objects that have not previously seemed electronic at all are starting to be online with embedded sensors and microprocessors, communicating with each other and the Internet. This includes several items such as food, clothing, household appliances, materials, parts, subassemblies, commodities, luxury items, landmarks, buildings, and roads.

It is estimated that 5% of human-constructed objects currently have embedded microprocessors [2]. These tiny microprocessor chips and sensors record and transmit data such as sound waves, temperature, movement, and other variables.

Cisco estimates that by 2020 there will be 50 billion connected devices, 7 times the world’s population [3]. Other sources such as; the Connected Life initiative sponsored by the GSMA (GSM Association) estimates that in 2020 there will be 24 billion total internet connected devices [4].

The IOT can be characterized by market segment; where exists three main categories: monitoring and controlling the performance of homes and buildings, automotive and transportation applications, and health self-tracking and personal environment monitoring.

Several papers addressed the issue of modifying internet of things (IoT) layered architecture. In paper [5], introduces a conceptual model for adaptive internet of things (IoT) communications that facilitates the identification of opportunities for adaption in each layer of the network stack by considering sharing information across layers to facilitate adaptation for heterogeneous devices.

In [6], a community health service architecture based on the internet of things (IoT) architecture is proposed for health care. The community health service technical architecture consists of three layers: Information perception layer, network transmission layer, and application layer. The motive behind this model is to enable doctors to monitor the health of patients remotely and in-real time to provide timely assistance whenever required. The Perception layer includes different types of sensors such as wearable sensors to detect the physical condition of the various organs and special sensors to detect the position of the user. Information collected from these sensors is sent to the wireless receiver and from there is transferred to the computer. From the PC data is transferred to remote health care monitoring center via the Internet. Application service layer combines the technology of IoT and medical health care center resulting in remote health service. Remote monitoring health care service improves cost savings and prevents overcrowding of hospital beds.

In [7], a three-layer network architecture for smart grid applications is proposed. The architecture is divided into the perceived extension layer, network layer and the application layer. The Smart Grid is termed as the 'the central nerve system' of the power system. Smart Grids can improve energy efficiency, reduce the environmental impact, improve the safety and reliability of electricity supply, and thus, reduce the electricity transmission of grid [8]. This IoT architecture for smart grids must include the four major modules of transmission, distribution, smart substations and the efficient usage of electricity for the smart grids.

Other papers [9], addressed the issue of securing the internet of things (IoT) because without strong security foundations, attacks and malfunctions in the internet of things (IoT) will outweigh any of its benefits. Traditional protection mechanisms – lightweight cryptography, secure protocols, and privacy assurance – are not enough. To implement internet of things (IoT) security measures successfully: understand the IoT conceptually, evaluate Internet security's current state, and explore how to move from solutions that meet current requirements and constraints to those that can reasonably assure a secure IoT.

In this paper, some modifications were proposed to the traditional Internet of things layered architecture. In the second section of this paper, the Internet of Things traditional architecture is illustrated, and the internet of things (IoT) common characteristics were clarified. In the third section of this paper, the proposed architecture is illustrated and explained in details. Finally, in the fourth section, conclusions and future work are discussed.

Internet of Things architecture and characteristics

Internet of Things (IoT) architecture. The internet of things give solutions based on the integration of information technology, which refers to hardware and software used in storing, retrieving, and processing data and communications technology which includes electronic systems used for communicating between individuals or groups. The fast convergence of information and communications technology is built on three layers of technology innovation: the cloud, data and communication pipes/networks and device [10].

As a result of this convergence, the IoT applications require the adaptation of classical industries and the technology will provide opportunities for new industries to emerge and to deliver new user experiences and services.

Besides, handling the sheer number of things and objects that will be connected in the IoT, cognitive technologies and contextual intelligence are important. This applies for the development of context aware applications that require reaching the edges of the network through smart devices that are included into everyday life.

The internet is not simply a network of computers, but it has evolved into a network of devices of all types and sizes, vehicles, smartphones, home appliances, toys, cameras, medical instruments and industrial systems, all connected, all communicating and sharing information all the time.

In Fig.1 [11], the internet of things layered architecture is illustrated as supposed by the ITU-T (International Telecommunications Union - Telecommunication Standardization Sector) and is composed of four layers; the top or first layer is the IOT application layer which contains the application user interface, the second layer is the services and application support layer, the third layer is the network layer which contains the networking and transport capabilities, the bottom layer is the device layer, which contains the gateways and the hardware and sensors and RFID tags and others. Along the four layers, the security and management capabilities and functions are distributed.

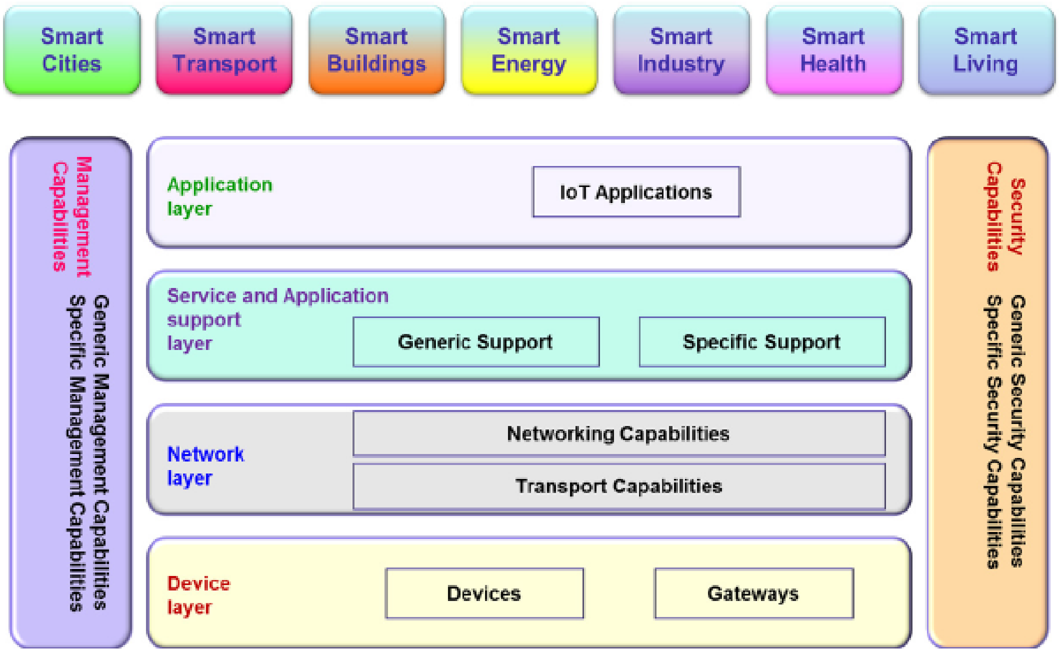

Fig.1. IoT layered Architecture (Source: ITU-T)

The internet of things is a universal concept and needs to be defined in a common way. Taking into consideration the huge background and diverse required technologies, from sensing device, communication subsystems, data aggregation and pre-processing to the object instantiation and finally service provision, generating a clear definition of the "Internet of Things" is not simple.

The IERC is very active in the involvement in ITU-T Study Group 13, which presents the work of the International Telecommunications Union (ITU) on standards for next generation networks (NGN) and future networks and has been working in the team which made the following definition for the Internet of Things [12]: "Internet of things (IoT): 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. NOTE 1- Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled. NOTE 2- From a broader perspective, the IoT can be perceived as a vision with technological and societal implications."

The IERC definition [12] defines the IoT as "dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network."

In Fig.2 [12], the IERC gives a detailed IOT Layered architecture, illustrating the functions included in every layer. In the topmost layer; the application layer, there is the application user interface. In the second layer, the service support and application support layer, some functions exists such as; IOT Business Process Management functions; which includes Business Process Modeling and Business Process Execution, Service Organization functions; which includes Service Composition and Service Orchestration, Virtual Entity functions; which includes VE Resolution, VE service and VE & IOT service monitoring, and finally, IOT service resolution and IOT service functions. In the third layer, the network and communication layer, there exists the network and communication capabilities, such as; Gateway, Routing and addressing, Energy Optimization, QoS (Quality of Service), Flow Control and Reliability, and error detection and correction. In the bottom layer, the Device layer, there exist the hardware components, the sensors, the RFID tags and other sorts of devices. In the left side, the Management Capabilities, such as; QoS Manager and Device Manager, are distributed along the service support and application support layer and the network and communication layer. In the right side, the Security Management functions, such as; Authorization, Key Exchange and Management, Trust and Reputation, Identity Management and Authentication, exists in the service support and application support layer and the network and communication layer.

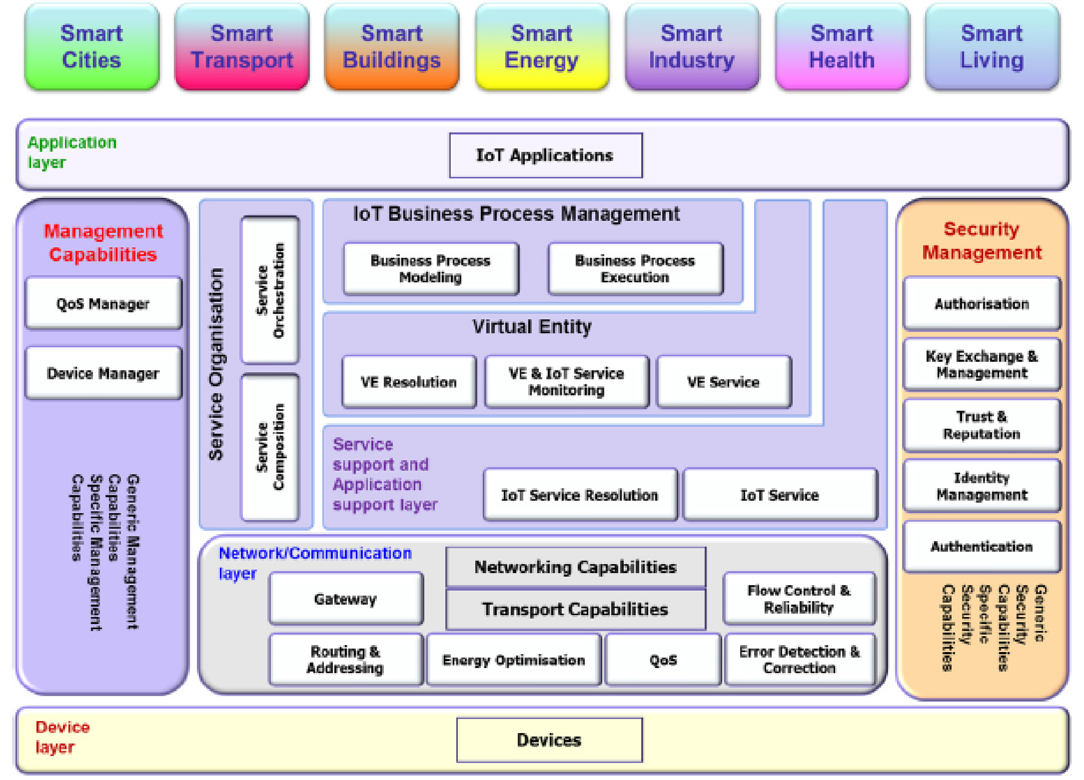

Fig.2. Detailed IoT Layered Architecture (Source: IERC)

The market designed for wireless communications is a very fast growing segment in the integrated circuit industry. Very fast innovation, rapid changes in communications standards, the entry of new players, and the evolution of new market sub segments will result to disruptions across the industry. LTE and multicom solutions increase the pressure for industry consolidation, while choosing between the ARM and x86 architectures forces players to make big steps that may or may not pay off.

Integrated networking, information processing, sensing and actuation capabilities give physical devices the ability to operate in changing environments. Tightly coupled cyber and physical processes of such systems are tightly interconnected and coordinated to work together in an effective way, with or without the humans in the cycle. Robots, intelligent buildings, implantable medical devices, vehicles that drive themselves or planes that automatically fly in a controlled airspace, are some of the examples of cyber-physical systems that could be entered in the Internet of things ecosystems.

IBM gave an illustrative IOT Landscape clarified in Fig.3 [13]. The IOT Landscape in Fig.3 divided the commercial applications on all the layers of the IOT traditional architecture. In the Connectivity area connecting the Device layer to the internet; there exists, USB, Wireless, PLC, RJ45, SP1 and other ways of connection. In the Link Protocol Layer, inside the network and communication layer, there exists GSM, CDMA, 802.15.4a, Ethernet, Bluetooth, Zigbee, Wi-Fi, 802.11 and other sorts of connecting networks. In the transport session, there are IPv4, IPv8, APL and other sorts of transport protocols. In the communication session, there are FTP, HTTP, SSH, Telnet, XMPP, DOS, MQTT and other sorts of communication protocols and softwares. In the service support and application support layer, the Data Aggregation/Processing can be done through some programs, such as; Scribe, Storm, Kaka, RapidVQ, Rume and others. The Data Storage and retrieval can be done through some programs, such as; MongoDB, Cassandra and others. The Business model can take one of these forms, such as; Open, Indirect, Integrated, Cloud, On-demand, Direct, Closed and others. In the application layer, there can be different types of applications, in the Device Management area, exists some programs for Firmware management, Remote Control, Device Registration, Device Provisioning, and others, in the Business Processes area, there are some programs that perform the following functions, Support, Marketing and Efficiency and others, in the area of analytics, there exists some programs for, Visualization, Data Analysis, Machine Learning, Data Mining and others. The security and Privacy functions are distributed along the four layers of the IOT architecture.

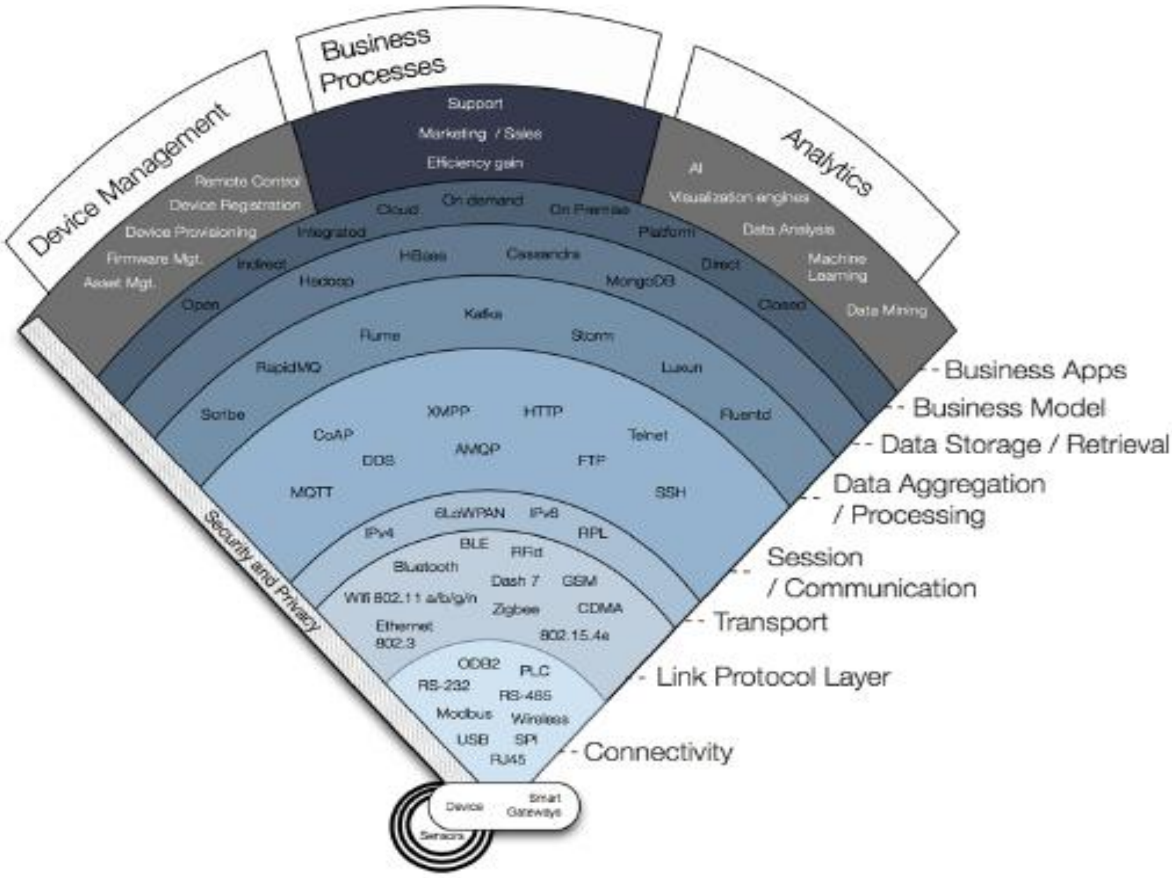

Fig.3. IoT Landscape [13]

Internet of Things (IoT) characteristics. Fig.4 [12] illustrates how everyday things are connected to a Wi-Fi network, each having a unique IP address that characterizes it. The objects connected to the Wi-Fi network, range from application PC, Application servers, PC, Biomedical equipment, scanner, printer, smart mobile device, tablet, laptop, video Camera, IP telephone, healthcare devices, vehicles to RFID readers and tags , wireless sensor nodes connected to a wireless gateway.

Fig.4. IP Convergence [12]

Ten "critical" trends and technologies affecting IT for the next five years were proposed by Gartner Group [14] and among them the Internet of Things. All of these things have an IP addresses and can be tracked. The Internet is expanding into enterprise assets and consumer items such as cars, televisions and others. The problem is that most enterprises and technology vendors are beginning to explore the possibilities of expanding Internet and are not operationally or organizationally ready to deal with these possibilities.

These possibilities can be applied to people, things, information, and places, and therefore the concept of "Internet of Things" will be followed by the concept of "Internet of Everything [15]."

In this context the concept of network convergence using IP is essential and depends on the use of a common multi-service IP network that supports a wide range of applications and services. Using IP to communicate with and control small devices and sensors enable the convergence of large, IT-oriented networks with real time and specialized networked applications.

The fundamental characteristics of the IoT as defined by IERC are as follows [12]:

Interconnectivity: With regard to the IoT, anything can be interconnected with the global information and communication infrastructure.

Things- related services: The IoT is capable of providing thing-related services within the constraints of things, such as privacy protection and semantic consistency between physical things and their associated virtual things. In order to provide thing-related services within the constraints of things, both the technologies in physical world and information world will change.

Heterogeneity: The devices in the IoT are heterogeneous as based on different hardware platforms and networks.

Dynamic changes: The state of devices change dynamically, e.g., sleeping and waking up, connected and/or disconnected as well as the context of devices including location and speed. Moreover, the number of devices can change dynamically.

Enormous scale: The number of devices that need to be managed and that communicate with each other will be at least an order of magnitude larger than the devices connected to the current Internet. The ratio of communication triggered by devices as compared to communication triggered by humans will noticeably shift towards device-triggered communication. Even more critical will be the management of the data generated and their interpretation for application purposes. This relates to semantics of data, as well as efficient data handling.

Proposed Improved Layered Architecture for IoT

In this paper, an improved layered architecture for internet of things (IOT) is proposed. This improved layered architecture depends on seven layers, not on four layers as the traditional layered architecture, and takes all the functions of the traditional architecture and distribute them on the seven layers, but in a more reliable way. The proposed improved layered internet of things (IoT) architecture composed of seven layers, is illustrated in Fig.5, as follows:

1- **Application layer:** includes the IoT application. This layer is at the top of the architecture and is responsible for delivery of various applications to different users in IoT. The applications can be from different industry segments such as: manufacturing, logistics, retail, environment, public safety, healthcare, food and drug etc. With the increasing maturity of RFID technology, numerous applications are evolving which will be under the umbrella of IoT.

2- **Application support & management layer:** performs the following functions; Qos Manager – Device Manager – Business Process Modeling – Business Process Execution – Authorization – Key Exchange & Management – Trust & Reputation - Identity Management. In this layer, all actions related to the control, security and management of the application are made.

3- **Services layer:** performs the following functions; Service storage & orchestration – Service composition & organization – Virtual Entity resolution – IoT service – VE service – IoT service resolution – VE & IoT service monitoring. All decisions related to the monitoring, storage, organization and visualization of the received information, including resolving virtual entities created, are made.

4- **Communication layer:** performs the following functions; Flow control & Reliability – Qos – Energy Optimization. Also, it performs cross platform communication, if required. The IoT web portal is in this layer. All decisions related to communications and measurements of the flow and its quality and energy consumed are made in this layer.

5- **Network layer:** performs the following functions; Gateway – Routing & Addressing – Network Capabilities – Transport Capabilities – Error detection & Correction. Also, it takes care of message routing, publishing and subscribing. With demand needed to serve a wider range of IOT services and applications such as high speed transactional services, context-aware applications, etc, multiple networks with various technologies and access protocols are needed to work with each other in a heterogeneous configuration. These networks can be in the form of a private, public or hybrid models and are built to support the communication requirements for latency, bandwidth or security.

6- **Hardware layer:** includes sensors, other hardware such as; embedded systems, RFID tags and readers and others. The sensors enable the interconnection of the physical and digital worlds allowing real-time information to be collected and processed. The miniaturization of hardware has enabled powerful sensors to be produced in much smaller forms which are integrated into objects in the physical world. There are various types of sensors for different purposes. The sensors have the capacity to take measurements such as temperature, air quality, movement and electricity. In some cases, they may also have a degree of memory, enabling them to record a certain number of measurements. A sensor can measure the physical property and convert it into signal that can be understood by an instrument. Sensors are grouped according to their unique purpose such as environmental sensors, body sensors, home appliance sensors and vehicle telemetric sensors, etc. Many of these hardware elements provide identification and information storage (e.g. RFID tags), information collection (e.g. sensors), and information processing (e.g. embedded edge processors).

7- **Environment layer:** includes objects to be detected or places to be observed. The objects to be detected vary from physical moving objects, such as humans, cars, to environmental factors such as, temperature, or humidity. The places to observed are ranging from buildings, universities, streets and so on.

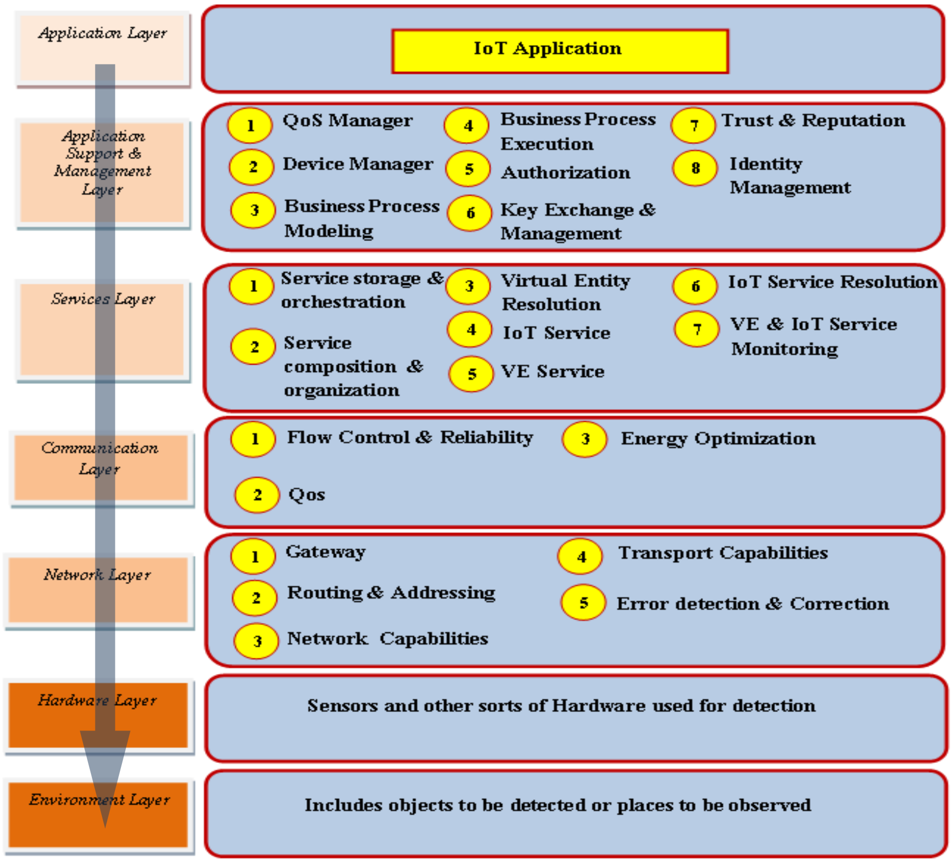

Fig.5. Improved Layered Architecture for IoT

Fig.6 shows how the seven layers interact with each other inside the proposed improved layered architecture for the internet of things (IoT). The interaction between layers can occur in both directions in some cases. First, the authorized person must provide his identity to the application, if the identity is right and registered in the IOT database in the services layer, he can open the application and request the information he wants. The environment layer includes objects to be tracked or places to be observed. The objects to be tracked are not usually static, they can move, for example, vehicles, also, the places to be observed, such as buildings, can contain movable objects or walking people. The hardware layer, includes the hardware components, such as; sensors, tracking devices, RFID readers and tags and others that transport live information about the tracked object or place to the network layer, which includes the multiple networks with various technologies and access protocols, such as, Wi-Fi, Ethernet, CDMA , GSM, Bluetooth and others. Then, the network layer take this live information to the communication layer, where the IOT Web portal resides, and performs cross platform communication using different protocols, such as, HTTP, FTP and others. The communication layer transmit this live information to the services layer, where all decisions related to the monitoring, storage, organization, resources allocation and visualization of the received information, including creating virtual entities, are made. Then, the received information is transmitted from the services layer to the application support and management layer, where it goes to the authorized person to receive this information. And finally, in the application layer, when the authorized person sitting before the application user interface receives this information, he must take the required decisions and also can request additional information from the application.

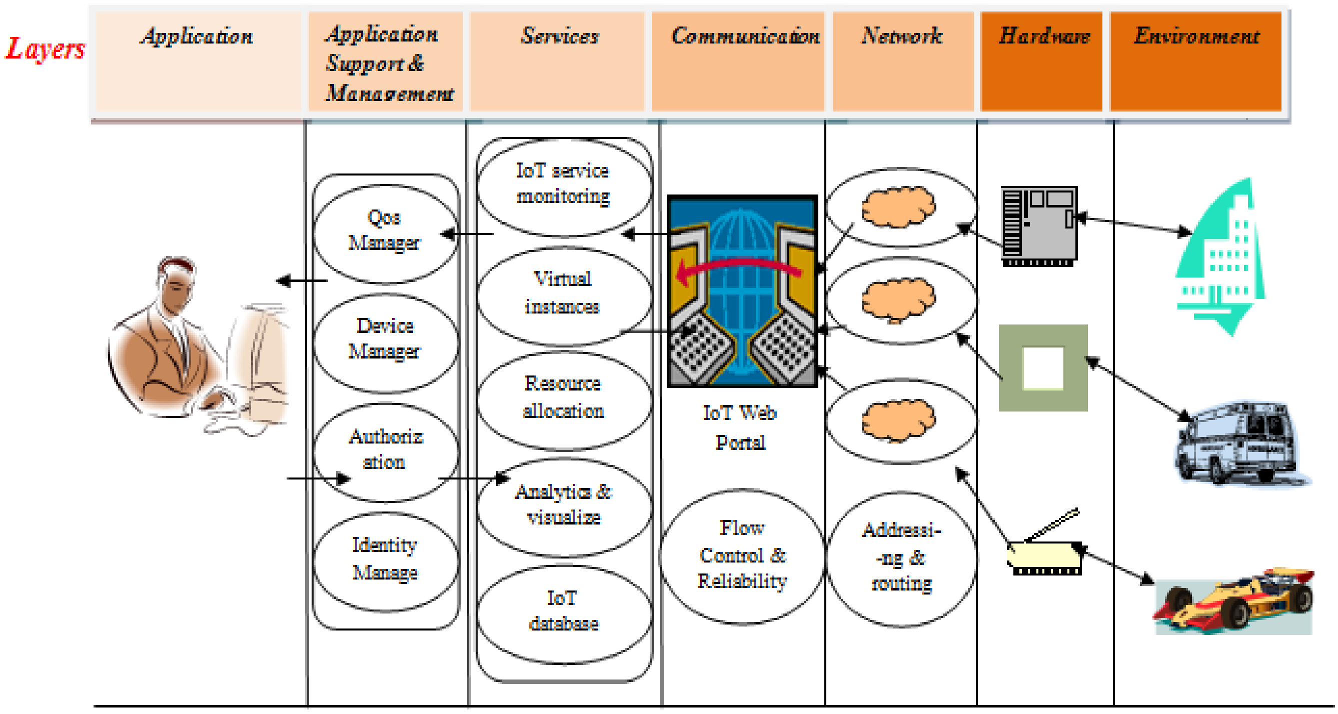

Fig.6. A model of end-to-end interaction between various layers in improved layered IoT architecture

Conclusion and future work

A more reliable Internet of Things (IoT) architecture is proposed in this paper. The proposed improved layered architecture of Internet of Things (IoT) is composed of seven layers and the environment layer is included in this architecture, and there is a sort of functions distribution on each layer. This proposed improved layered internet of things architecture differs from the traditional internet of things (IoT) architecture by its reliability and feasibility to all sorts of applications, also, it is more flexible. In the future work, there will be a focus on building new model applications for internet of things (IoT) based on this proposed internet of things (IoT) architecture.

References

[1] US National Intelligence Council, (2008) "Disruptive Technologies Global Trends 2025: Six Technologies with Potential Impacts on US Interests Out to 2025". [Online]. Available: http://www.fas.org/irp/nic/disruptive.pdf.

[2] Vinge V., (13 – 14 Oct. 2012) "Who's Afraid of First Movers?", The Singularity Summit, San Francisco, CA, USA. [Online]. Available: http://singularitysummit.com/schedule/.

[3]Evans D., (2011) "The Internet of Things", Cisco Blog. [Online]. Available: http://blogs.cisco.com/news/the-internet-of-things-infographic/.

[4] Brand T., (2012) "Connected Living: The Next Wave of Mobile Devices", GSMA Ministerial Programme. [Online]. Available: http://www.gsma.com/connectedliving/wp-content/uploads/2012/05/thenextwaveofmobiledevices.pdf.

[5] Peng Du and George Roussos, "Adaptive Communications Techniques for the internet of things", Journal of sensor and actuator network, 6 Mar. 2013.

[6] Wu-Zhao, Liu Lei-hong, Huang Yue-shan and Wu Xiao-ming, "A Community Health Service Architecture Based on the Internet of Things on Health-Care", World Congress on Medical Physics and Biomedical Engineering, vol. 39, pp.1317-1320, 2013.

[7] Ling Zheng, Shuangbao Chen, Shuyue Xiang and Yanxiang Hu, "Research of Architecture and Application of Internet of Things for Smart Grid", Computer Science & Service System (CSSS), 2012 International Conference, pp.938-941, 11-13 Aug. 2012.

[8] Li Li, Hu Xiaoguang and Chen Ke; He Ketai, "The applications of WiFi-based Wireless Sensor Network in Internet of Things and Smart Grid", Industrial Electronics and Applications (ICIEA), 2011 6th IEEE Conference, pp.789-793, 21-23 June 2011.

[9] Rodrigo Roman, Pablo Nagero, and Javiez Lopez, "Securing the internet of things", Article published in IEEE Computer, vol.44, no. 9, Sept. 2011, p.51-58.

[10] Danh Le Phuoc, Martin Serrano, Hoan Nguyen Mau Quoc and Manfred Hauswirth, "A complete stack for building Web-of-Things Applications", submitted to the IEEE Computer Systems Journal, Special issue on the Web-of-Things 2013, 2013.

[11]International Telecommunication Union – Telecommunication Sector, "Series Y: Global Information Infrastructure, Internet Protocol Aspects and next Generation Networks - Frameworks and functional architecture models - Overview of the Internet of things, Y.2060", June 2012.

[12] Ovidiu Vermesan and Peter Friess, "IERC Cluster SRIA 2014 – Internet of Things – From Research and Innovation to Market Deployment", River Publishers Series in Communication, 2014.

[13]IBM Software Group, "Breaking through the haze: under-standing and leveraging cloud computing", Route 100, Somers, NY, U.S.A., 2008.

[14] (5-9 Oct. 2014) Gartner Symposium/ITxpo 2014, Orlando, USA. [Online]. Available: http://www.gartner.com/newsroom/id/2867917/.

[15] Dave Evans, (2012) "The Internet of Everything: How More Relevant and Valuable Connections Will Change the World", Cisco Internet Business Solutions Group (Cisco IBSG). [Online]. Available: https://www.cisco.com/web/about/ac79/docs/innov/IoE.pdf