Internet of Things - Architecture, Applications Challenges,and A way to Standardization

Nadia Salem
The Univirsity of Yarmouk , Irbid, Jordan, Prince Faisal Information Technology,
Nsalme01@nyit.edu
Asma Salem
The University of Jordan, Amman, Jordan,King Abdullah II School of Information Technology,
Asma_salem85@yahoo.com
Ayat M. Salem
Ministry of Information and Communications Technology/E-government, Amman, Jordan,
ayat.salem @moict.gov.jo

Abstract— In this paper, we are going to explain the Internet of Things' (IOT) its Definition, recent history, Architecture, Applications, and technological challenges. We will also conclude by Issues to be addressed.

Keywords—Internet of Things, Standard, RFID, Sensors, Wireless Sensors. Cloud computing.

1. INTRODUCTION

Internet Of Things (IOT) is recently considered to be the next evolution of the internet, using this development of the internet, it become too easy to gather, analyze, distribute data and turn it into information. Then to knowledge, and finally, to wisdom.

All the technology trends aim to make an evident enhancement added to human's life by transforming the data from being insignificant object, presented anywhere, taken from anyone, about anything, and originated from Anything or Anyone. elaborating data to build blocks of information ,which could be used by engineers ,experts and researchers then combining the information with the intelligent parts and objects to get a big knowledge from them ,thus it will improve the Quality of human's life by using the highest level of the IOT which is wisdom .

These phases of the data improvement are demonstrated, by Fig (1) below.

Fig (1) .Wisdom ,Knowledge ,Information, Data paradigm

because of the fact that, data is the foundation stone to the internet information flow, the IOT is considered to be the essential (producer /consumer) part of this data flow, as a result of that, the IOT allows people and things to be connected at Any time or in Anyplace or about Anything or with Anyone. And this by using any path/network, to get Any service we want [4][5][7].

In this paper we try to highlight the definitions and the visions of the IOT ,also we try to show the different perspectives that are being used to find the suitable definitions for the IOT evolution, we are going to go through the definition s and visions in the section(2),the history will be demonstrated in section(3),application and architecture will be discussed in section (4) and (5) respectively ,in section (6) the technology is described in details ,and we will go through the challenges in section (7),leaving the challenges with some open issues and the conclusion in section (8) and (9) .

2. IOT Definition and vision

In research communities, the IOT has been defined based on different perspectives ,as a result of that the IOT has numerous definitions in literature. And today's plain fuzziness in relation IOT term comes as a consequence to the name (Internet of Things) itself.

If we think about the definition of IOT, we will conclude that it is one paradigm with different meanings. along with the IOT history, the definition is Changed according to

different perspectives, the first definition is derived from the "things oriented" perspective, the second definition is derived from "internet oriented" perspective ,while the third definition is derived from "semantic oriented visions" ,and this might lead us to the most recurrent definition which is defined according to the European commission as "Things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts" [4] [7].

Thus the most comprehensive definition is : things and objects will communicate with each other, and interact by using all available technologies to deliver the needed information in the exact time and suitable situation.in other words, to let the things have the ability to think and make decision [4][5][7] .

There are Different applications to be derived from the comprehensive vision of the definition as it described in the Fig(2),the 6A paradigm appears here (Anything, Anytime, Anyone, Anyplace, Any service, Any network)all of these factors will contribute with each other's [4].

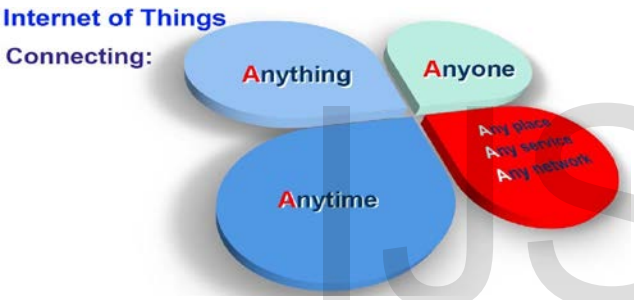

Fig (2) IOT will cover everything, 6 A connectivity

The IOT Umbrella Concept compromises all the technologies such as communications ,networking, computing and software engineering solutions for (anywhere, anytime and by anything) ,by comprehensive thinking we can figure out that the IOT isn't a new brand class of systems ,but it extends the ICT systems/applications , by providing additional functionalities in relation to the sensing ,and interacting with the physical realm [2][4].

This is leads us to its main rule, which is to use the existing networks along with the internet to do its job. According to the one business perspective , the IOT is an investment to the idea implementation and realization, on the other hand ,according to system perspective sides using the IOT may result in some challenges in relation to the heterogeneous networks with many different types and various related details concerning technologies and protocols, that need to communicate ,explore and elaborate each other's, along with the realm [2] .

3. History

The Internet of Things term is coined by Kevin Ashton, the executive director of the Auto-ID Center in 1999, According to Cisco Internet Business Solutions Group (IBSG), the Internet of Things was born in between 2008 and 2009 at simply the point in time when more "things or objects" were connected to the Internet than people [5].

Citing the growth of smartphones, tablets, PCs, … etc the number of devices connected to the Internet was brought to 12.5 billion in 2010, while the world's human population increased to 6.8 billion, making the number of connected devices per person more than 1 (1.84 to be exact) for the first time in history. Shown in the Fig (3) [1][5].

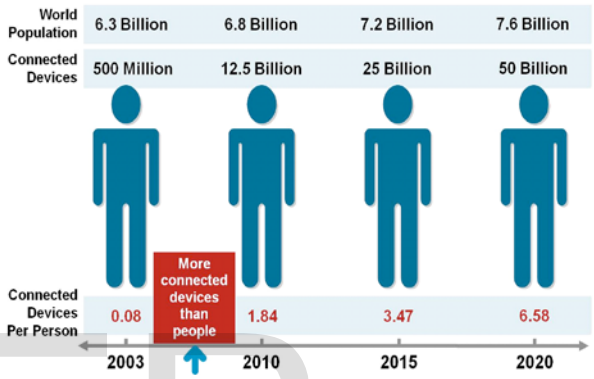

Fig (3): statistical information for connected devices per person2003-2020 and the year IOT has born

4. Applications

Moving towards the heterogonous environment, which the internet of things can work in, we could offer potentials possibilities for development of huge number of applications, which is already a small part from our world we live in, & many others would improve the quality of the life whatever whenever we are.

When we are equipped our environment with the intelligence objects & giving these parts ability to communicate with each other's , adding the value of being transmitting & receiving information ,we get many applications bolded under the following domains :-
(a)Transportation and logistics domain. (b) Healthcare domain. (c) Smart environment (home, office, plant) domain. (d) Personal and social domain. [4][7].

5. IOT-A Architecture

A layered model for IOT-A architecture is the suitable design that meet different requirements of the heterogeneous systems , various environments , societies , governments and distributed resources ,IOT-A consists of these major layers with internet layer devising them:

1-Edge Technology layer: it is consist of different technologies used in IOT-A, and involve all hardware devices and entities that provide different services.

2-Access gate way layer: the first stage of data handling.

3-Middle ware layer : this is the most critical one because it operates in bidirectional mode, it is an interface between the application and technological layers , the best advantage of this layer is the hiding of all the technological details from the programmers , simplifying the development process of the applications needless for knowing the details of the lower layer .
In addition, this layer follow the service oriented architecture approach (SOA), using some common interfaces and standard protocols, making another horizontal view of a good system.

4-Application layer: this is the top layer of the IOT-A layered model; it is representing all the applications that refer to different users and also for different industries.

Finally, the IOA architecture must be performed under some conditions, Distributed open architecture with end to end characteristics, interoperability of heterogeneous systems, neutral access, clear layering and resilience to physical network disruption, and Decentralized autonomic architectures based on peering of nodes [4][7][8].

6. Technology

In term of enabling technologies, the IOT is the appropriate development factor for identifying smart objects and enabling interactions with the environment.

6.1 IOT key Technology

The key building blocks are expected to be used by wireless sensor networking technologies, and radio frequency identification devices RFID and as well as the smart objects indeed.

Although there is no an existing standard to cope with this huge different complete technologies, we wish to reach the perfect standard that will rise the quality of service of the IOT as soon as to fulfill the dream of being real and applicable.

6.1.1 Radio Frequency Identification (RFID)

RFID (Radio Frequency Identification) is primarily used to identify objects from a distance of a few meters, with a stationary reader typically communicating wirelessly with small battery-free transponders (tags) attached to objects. Which helps in the automatic identification of anything they are attached to acting as an electronic barcode [7].

There are different types of RFID, the passive RFID tags, which are not battery powered, and the Active RFID tags, which have their own battery supply and can instantiate the communication. We will summarize the differences in table (1) [2][7].

RFID technology is expected to play a key role as enabling identification technology in IOT providing two important functions in the Internet of Things – identification and communication – RFID can also be used to determine the approximate location of objects provided the position of the reader is known [1][7] .

Comparison element/Type	Active RFID	Passive RFID
Power	Battery operated	No internal power
Required Signal Strength	Low	High
Communication Range	Long range (100m+)	Short range (3m)
Range Data Storage	Large read/write data (128kb)	Small read/write data (128b)
Industries/Applications	Auto dealerships, Auto Manufacturing, Hospitals – asset tracking, Construction, Mining, Laboratories, Remote monitoring, IT asset management	Supply chain, High volume manufacturing, Libraries/book stores, Pharmaceuticals, Passports, Electronic tolls, Item level tracking

Table (1) Comparison of Active and Passive RFID

6.1.2 Smart Objects:

Smart Objects represent the capabilities of objects participating in the IOT, from the basic capacity to provide a unique identification number to more complex abilities such as the capacity to perform networking and decision-making.

The Smart Objects provide services to end-users such as identification and condition information through a well-defined set of interfaces. And this information will be organized in such a way to allow user access with various degrees of granularity [3].

The smartphone now is no longer just a device, but it's actually going to be the platform for the Internet of Things, people are going to have all these fancy new devices that they can control from their smartphones. Moving from network of interconnected computers to a network of interconnected objects [6].

Technology	Processing	Sensing	Communication	Range (m)	Power	Lifetime	Size	Standard
RFID	No	No	Asymmetric	10	Harvested	Indefinite	Very small	ISO18000
WSN	Yes	Yes	Peer-to-peer	100	Battery	<3 years	small	IEEE 802.15.4
RSN	Yes	Yes	Asymmetric	3	Harvested	Indefinite	Small	None

Table(2) comparison between technologies (RFID ,WSN,RSN)

6.1.3 Wireless Sensor Networks (WSN)

The Internet of Things infrastructure allows multiplexing of smart objects (i.e., wireless sensors, mobile robots, etc.), sensor network technologies, and human beings, using different communication protocols, thus it will create a dynamic heterogeneous network that can be deployed.

In this infrastructure, these different entities or "things" discover and explore each other and learn to take advantage of each other's data by pooling of resources and dramatically enhancing the scope and reliability of the resulting services.

Sensor networks consist of a certain number (which can be very high) of sensing nodes communicating in a wireless multi-hop fashion. Usually nodes deliver the results of their sensing to a small number (in most cases, only one) of special nodes called sinks. large scientific works have been done on sensor networks in the recent past; addressing several problems at all layers of the protocol stack as we will discuss these challenges in the challenge's section [7] .

Sensor networks play an important role in the IOT. They can work together with RFID systems, to introduce a new technology RSN (Radio Sensor Network), which will give us the ability to track the status of things, i.e., their location, temperature, movements, …,etc.
RNS could act as a further bridge between physical and digital world. Usage of sensor networks has been proposed in several application cases, such as environmental monitoring, e-health, intelligent transportation systems, military, and industrial plant monitoring. [2][4][7] .

6.2 Technologies standards and Protocols:

IOT will be characterized by large heterogeneity in term of devices, taking parts in the system, which will present very different capabilities from computations and communications standpoints, the management of such high level of heterogeneity should be supported at both architecture and protocols levels [2][7].

Table (2) compares the characteristics of RFID systems (RFID), wireless sensor networks (WSN), and RFID sensor networks (RSN). Observe that the major advantages of:

_ RFID are the smallest in size and the cheapest in cost, & their lifetime is not limited by the battery duration (RFID passive tags).

_ WSN are the highest in relation to the radio coverage and the communication paradigm, which does not require the presence of a reader (communication is peer-to-peer).

_ RFID sensor network are the possibility of supporting sensing, computing, and communicating capabilities in a passive system [7].

6.3 The Internet in the Internet of Things

In the IOT there is a need for substantial progress in research achievements at several fields. First, today there is no single way of identifying an object in the internet of things: there are several standards, such as 2-D bar codes, GS1, uID, IPv6 addresses, but they are non-compatible. Moreover, reference architectures which can lead the way to any kind of real-life system implementation must be identified and standardized. [8].

Today, several communication mechanisms are deployed in current applications, and any novel technologies will need to guarantee interoperability between different protocols. We must also consider that the lifetime of network technologies might be much shorter than the one of the physical objects connected to it, and where the same technology is applied.

In the "common" internet, the interoperability between low-layer technology and services is assured by the use of the Internet Protocol (IP). Usually, the network technologies are represented in an hourglass shape, with the IP layer in the middle, and this is commonly referred as 'the narrow waist' of internet. *The questions of what shape the IOT 'narrow waist' will have - and even if such a thing will exist*, considering the heterogeneity of IOT technologies, are of primary importance, and future research should clearly focus on them.

We are going to sum up the different physical communication interface types, with several communication types and the Required protocols, depending on their distribution at different OSI layers /internet stack protocol [4][7][8], in table (3) below:

Physical Communication	Communication Type	Protocols	OSI Layers

Interface Type			
802.15.X series (Zigbee,Blue tooth, RFID, etc)	Wireless Wireless	NWK/APS/API defined by each standard isation body (all non-IP)	Network Transport Upper
WIFI	Wireless	IP-TCP/UDP	Network Transport Upper
Sensor network busses	Fixed	up to data link	data link
Ethernet/IP	Fixed	IP-TCP/UDP	Network Transport Upper

Table(3) :communications type and protocols

7. Challenges:

The key point behind the IOT concept, resides in the huge potential of embedding computing and communication capabilities into objects of common use, leads our thinking of many challenges face the implementation of the idea in the real world, first of all :

7.1 standardization

Until now we are considering IOT under the open standard, in which there are many studies and researches to move towards the global standard which will serve the technology in such ways.

We are interested here to show some of these challenges in order to design a comprehensive standard, since the frame works of these studies and researches are huge, detached from a united comprehensive complete vision.

7.1.1 IOT minimum requirements

The parts which represent the building block in the IOT such as devices, smart objects and anything must have some common features which will enable them to be identified, interact and communicate between the real and virtual world. Starting from being a device need to be attached will be having the minimum requirements [4] ,and this leads to many challenges ,we summarize the most of them in the following table (4) : -

IOT Requirement	Research's and Standardizations fields needed
1. Have a physical embodiment and a set of associated physical features (e.g., size, shape, etc.)	hardware standard needed
2. Have a minimal set of communication functionalities.	Network and communication standard needed
3. Possess a unique identifier	Communications standards are needed
4. Are associated to at least one name and one address.	Naming and Addressing standard needed
5. Possess some basic computing capabilities, The ability to match an incoming message and complex computations, service discovery , network management tasks .	computations service model and architectural standard needed
6. May possess as to sense physical phenomena (e.g., temperature, light, …etc	Data and signal processing technologies and standard needed .

Table(4) :communications type and protocols

These challenges in different parts concerning the IOT requirements, open many issues needed to be addressed and create a comprehensive fields for the researchers and the experts [2][4][7].

7.1.2 IOT and TCP/IP inadequacy:-

With deep looking at IOT , each object that is a part of the IOT will arise different levels of challenges starting with : Naming , addressing as well as ending with the arguments about and open issues for researching in networking/routing standards and using the existing ones to serve the IOT needs , indeed returning to the existing network standards and protocols , we will discuss the challenges of being the TCP/IP protocol for example is inadequate for the IOT ,due to the following reasons :

1. Connection setup: the TCP three ways handshaking is not necessary in IOT , given that most of the communications within the IOT will involve the exchange of a small amount of data with a limitation of time and power [3][7].

2. *Congestion control*: TCP is responsible for performing end-to-end congestion control. In the IOT this may cause performance problems as most of the communications will exploit the wireless medium, which is known to be a challenging environment for TCP [7].

3. *Data buffering*: TCP requires data to be stored in a memory buffer both at the source and at the destination. In fact, at the source data should be buffered so that it can be retransmitted

in case it is lost. At the destination data should be buffered to provide ordered delivery of data to the application. Management of such buffers may be too costly in terms of required energy for battery- less devices [3][7].

4.*Traffic characterization*, we do not know what will be the characteristics of the traffic exchanged by smart objects in the IOT; Whereas it is fundamental to investigate such characteristics as they should be the basis for the design of the network infrastructures and protocols [7].

Up to date, no solutions have been proposed for the IOT and therefore, research contributions are required until now.

7.2Power and Energy:

While the IOT promises to connect billions of smart devices as we illustrated in Figure (3) , the need to ensure adequate power for the expected years of operation of these devices remains a challenge [5][7]

Almost all Internet of Things devices will be wireless due to the expense and inconvenience of wiring these devices. With no cord for data or power, these devices must be self-powered. There are only two ways internet of things devices can be powered [4][5]:
(a)The Non-rechargeable traditional battery that needs to be changed when exhausted or;(b) the Rechargeable battery using ambient energy harvesting that lasts the life of the product.
Energy-harvesting techniques offer a power solution well suited to the operating conditions expected for many of these smart devices. Using available ICs designed specifically for energy-harvesting applications, engineers can address emerging IOT applications with smart devices able to operate for years on ambient power sources including solar, temperature, vibration, and RF energy [3][4].
Recent advances in ambient energy transducers, rechargeable solid state batteries and high efficiency power conversion electronics are making Energy Harvesting-based power solutions cost effective. Energy Harvesting solutions are especially cost effective when the life cycle costs of changing batteries are taken into account [3].

7.3 Security

Internet of Things needs to be built in such a way as to ensure an easy and a safe user control. Consumers need confidence to use the Internet of Things in order to get its potential benefits and to avoid any risks to their security and privacy[4].

All the talking and complains following the announcement by the Italian retailer Benetton on the plan to tag a complete line of clothes (around 15 million RFIDs) has been the first, clear confirmation of this mistrust towards the use that will be done of the data collected by the IOT technologies [7]

The heterogeneity and the scalability of 'things' in the IOT will add complexity to adopting it, adding their mobility and often their relatively low complexity so the internet of things is hard to control.

In this section, we seek to revise and discuss the major security challenges to be addressed in order to turn Internet-of-Things technology into a mainstream.

In particular, we identified three key issues requiring innovative approaches: data confidentiality, privacy and trust. In the following, we analyze them one by one [2].

7.3.1 Data confidentiality

Data confidentiality represents a fundamental issue in IOT scenarios, indicating the guarantee that only authorized entities can access and modify data.

Data confidentiality may not be straightforwardly applied to IOT contexts, due to two major limiting factors. The first concern is the huge amount of data generated by such systems and relates hence to scalability issues. The second concern focuses on the need of controlling the access to data in an on-line and a flexible way, with access rights changing at run-time and being applied to dynamic data streams.

Summarizing, the main research challenges for ensuring data confidentiality in an IOT scenario relate to: Definition of suitable mechanisms for controlling access to data streams, another issue is to create of an appropriate query language for enabling applications to retrieve the desired information Out of a data stream, and of course of a suitable smart objects identity management system [4][7][8].

7.3.2 Privacy:

By ensuring that individuals can control which of their personal data is being collected, who is collecting such data, and when this is happening Privacy should be protected. Furthermore, the personal data collected should be used only in the aim of supporting authorized services by authorized service providers.

In conclusion, the open research challenges in terms of privacy preserving mechanisms for IOT are given by: Definition of a general model for privacy in IOT and Development of innovative enforcement techniques, able to support the scale and heterogeneity characterizing IOT scenarios [4][7][8].

7.3.3 Trust:
The main problem with many approaches towards trust definition is that they do not lend themselves the establishment of metrics and evaluation methodologies.

The most relevant research challenge in the definitions of appropriate trust mechanisms for IOT can be outlined as: (a)

Introduction of a simple trust negotiation language (b) Definition of a trust negotiation mechanism (c) Development of an adequate object identity management system (d) Design Of a general and flexible trust management framework [4][7][8].

8. Open Issues

8.1 Cloud Computing

Cloud computing has been established as one of the major building blocks of the Future Internet. New technology enablers have progressively fostered virtualization at different levels and have allowed the various paradigms known as "Applications as a Service", "Platforms as a Service" and "Infrastructure and Networks as a Service". [10]

Such trends have greatly helped to reduce cost of the ownership and the management of the associated virtualized resources, lowering the market entry threshold to new players and enabling provisioning of new services [1][8].

With the virtualization of objects being the next natural step in this trend, the convergence of cloud computing and Internet of Things, will enable IOT services fields to be As a part of this convergence , we summed up some of them in table (5) :-

Cloud/Virtualization layer	IOT virtualized part
Application layer	IOT applications (such as sensor-based services) Sensing-As-A service
Resources layer	"Object as a Service" aimed to virtualized resource domains.

Table(5) Cloud Computing with IOT

An integrated IOT and Cloud computing applications enable the creation of smart environments such as Smart Cities, which need to combine services offered by multiple services providers and to scale support of a large number of users in a reliable and decentralized manner, with limited power and unreliable connectivity [8][10].

The Cloud application platforms need to be enhanced to support a rapid creation of applications by providing domain specific programming tools and environments ,in seamless execution of applications dealing with capabilities of multiple dynamic and heterogeneous resources to meet quality of service requirements of numerous number of users [10][8].

8.2 Breaking the Unbreakable: The End-to-End Principle

The internet as we know it today is based on a few, very simple but very meaningful principles. One of these is the "end-to-end" principle: keeping the technologies in the network very simple and dealing with complexity at the end points only, allowing the Internet architecture to be very scalable [9].

With regards to the IOT domain, there might be a different point of view. It has to be considered up to what extent IP technology will be used. While many technologists believe that IP will finally be on each and every smart device there are many particular cases which show the likeliness that different solutions are necessary, shown in table (6).

Some TCP features	IOT scenarios
1-best-effort, connectionless, unreliable protocol	the real-time devices, such as the parking systems at cars, which cannot be based on the best-effort, connectionless, unreliable protocol (as the IP is, by definition)
2- complex protocol (IP)	the tiny, extremely cheap devices, (such as passive RFID tags) which may be stateless
3- TCP as a common language	smart devices do not necessarily need to speak the same language: a medical device such as a Nano robot, which is used to fight cancer cells in the human body, has totally different needs than those of a smart fabric needing to communicate its characteristics to a washing machine

Table(6) some TCP features Vs. IOT applications .

As the end points of IOT can be extremely simple (as a temperature sensor), even if they will be able to use the IP protocol it is unlikely that they will be able to deal with complexity.

Therefore, it is likely that, at some layer, there will be bridges between systems; and these bridges (or gateways) might be considered the end-to-end points between communicating entities. So between two different objects communicating, the communication path may be broken into different sections (object-to-gateway, gateway-to-gateway, and gateway-to-object) [7][9] .

There is a strong need to further investigation on this matter, and to come up with a commonly accepted set of founding principles [8].

Regarding to all these open issues and referring to the challenges we have in the last sections, we conclude that The engineering hurdles to the IOT center on solving the tough problems in security, standardization, network integration, ultralow-power devices, energy harvesting and, but the most

important of all, perceived network reliability, In order to make the IOT a reality.

The IOT will require the creation of servers far more powerful and intelligent than ones that are currently in operation, to create an effective system that will be able to collect and process the mass amounts of data will give off, Testing these servers may require a great deal of trial and error, which would consume a lot of time and cost a lot of money.

9. Conclusion

In conclusion, the Internet of Things is closer to be implemented than an average person would think. Most of the necessary technological advances needed for it have already been made, and some manufacturers and agencies have already begun implementing a small-scale version of it.

The main reasons why it has not truly been implemented until now in a comprehensive frame work ; are the huge impact which will leave in the legal, ethical, security and social fields, in addition to the energy harvesting fields challenging issues .

As a result of all , the Internet of Things need to be pushed back to the standardization of different processes in order to take the lead in our modern life, this is the potential issue should be in next year's agenda for the roadmap for the IOT .

10.REFERENCES

1. Gubbi, J., et al., Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 2013.
2. Miorandi, D., et al., Internet of things: Vision, applications and research challenges. Ad Hoc Networks, 2012. 10(7): p. 1497-1516.
3. López, T.S., et al., Adding sense to the Internet of Things. Personal and Ubiquitous Computing, 2012. 16(3): p. 291-308.
4. Vermesan, O., et al., Internet of things strategic research roadmap. O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, H. Sundmaeker, A. Bassi, et al., Internet of Things: Global Technological and Societal Trends, 2011: p. 9-52.
5. Evans, D., The Internet of Things: How the next evolution of the internet is changing everything. CISCO white paper, 2011.
6. Mattern, F. and C. Floerkemeier, From the Internet of Computers to the Internet of Things, in From active data management to event-based systems and more. 2010, Springer. p. 242-259.
7. Atzori, L., A. Iera, and G. Morabito, The Internet of Things: A survey. Computer Networks, 2010. 54(15): p. 2787-2805.
8. Ian,G. Smith, Ovidiu Vermesan ,Peter Friess , And Anthony Furness ,The Internet of Things 2012 New Horizons., IERC - Internet of Things European Research Cluster. 2012, p. 22-61.
9. Saltzer, Jerome H., David P. Reed, and David D. Clark. "End-to-end arguments in system design." ACM Transactions on Computer Systems (TOCS) 2.4 (1984): 277-288.
10. Ayat M. Salem , Feras S. Al-Shalabi and Mohamad M. AL-laham. "The Influence of Cloud Computing Adoption Challenges on e-Government Services A case study: Jordanian e-Government" International Journal of Scientific & Engineering Research, 2017. 8(7): p. 213.