Internet of Things (IoT): Definitions, Challenges and Recent Research Directions

Zainab H. Ali
Dept. of Computer Eng. &
Systems, Mansoura University,
Egypt.

Hesham A. Ali
Dept. of Computer Eng. &
Systems, Mansoura University,
Egypt.

Mahmoud M. Badawy
Dept. of Computer Eng. &
Systems, Mansoura University,
Egypt.

ABSTRACT

In this paper, we seek to highlight the concept of Internet of Things (IoT) in general, as well as reviewing the main challenges of the IoT environment by focusing on the recent research directions in this topic. Recently, IoT has emerged as a new technology that is used to express a modern wireless telecommunication network, and it can be defined as an intelligent and interoperability node interconnected in a dynamic global infrastructure network, also it seeks to implement the connectivity concept of anything from anywhere at anytime. Indeed, the IoT environment possesses a large spectrum of challenges has a broad impact on their performance, which can be divided into two categories, namely, i) General challenges: such as communication, heterogeneity, virtualization and security; and ii) Unique challenges: such as wireless sensor network (WSN), Radio Frequency Identification (RFID), and finally Quality of service (QoS) that is considered as a common factor between both general and special challenges. In addition, this paper highlights the main applications of the IoT.

Keywords
IoT; heterogeneity; virtualization; WSN; RFID; QoS.

1. INTRODUCTION
Today, we are living in the era of smart technologies which represents a "ubiquitous computing" or "web 0.3". Internet of Things (IoT) has emerged strongly as a more prosperous area to express this kind of a new technology. It is not the first technology in this field, but also the cloud computing technology has been used to represent the ubiquitous computing world. In the seventh in the series of ITU Internet Reports originally it was launched in 1997 under the title *"Challenges to the Network"* [1], and it was first coined by Kevin Ashton in the RFID journal 1999 [2], In 2005 this name was changed to "Internet of things". The vision of IoT according to Kevin's vision was to enable networked devices to propagate their information about physical world objects through the web. In recent years, the most of the IoT proposed architectures are used, web semantic to publish information through the social networks; for instance, the iPhone has innovated service is Nike + iPod to record information and published it on the social networks and the social network friends [3].

Actually, the definition of IoT varies based on who you talk, but formally, it can be defined as a dynamic global network infrastructure with self-configuration and interoperable communication. Simply, IoT means the ability to make everything around us starting from (i.e. Machine, Devices, Mobile phone and Cars) even (Cities and Roads) are expected to be connected to the Internet

with an intelligent behavior and taking into account the existence of the kind of autonomy and privacy. Meanwhile, the IoT environment contains a huge number of the different objects/things can be classified into two types namely; i) Things rechargeable batteries things: the most of them are mobiles (e.g. Laptop, tablets and mobile phone), and ii) Things are non-rechargeable things: these things are static from the mobility point of view [4]. Generally, IoT includes three main demands are: the first, a shared understanding of the situation of its users and their applications. Secondly, software architecture and pervasive communication networks to cover and process contextual information, and lastly, the analytics tools in IoT that aims for autonomous and intelligent behavior [5].

Considerably, can be expressed the principle idea of IoT is promoting the communication between anything from anywhere at anytime through context-aware applications. Accordingly, IoT has relied on RFID and sensor network technologies in the implementations. For instance, IBM company used IoT in Norwegian Sea oil platforms, by deploying sensors at seabed that are used to collect real information to make decision drill in the sea [3].
On the other hand, the IoT environment like many networks suffering from the set of challenges which significantly affect their performance some of them are common and others, are special; the paper divides these challenges into two categories, namely, *i) General challenges:* which include common challenges between IoT and traditional network such as communication, heterogeneity, QoS, scalability, virtualization, data mining and security; and *ii) Special challenges:* such as RFID and WSN.
The main objective of this paper provides an overview about IoT, its definition, its architecture, and discusses the differences between IoT and the traditional Internet; then highlighting the challenges of IoT and the recent research directions to solve them. Finally, the rest of this paper is summarized as follows: section II, introducing an overview about IoT concept, its history and its inception also discussing the differences between IoT and the traditional Internet; section III, focusing on the challenges and recent research directions to address them and section IV, reviewing a set of the most popular applications in IoT

2. Related Work
In this section, the paper seeks to offer a brief overview about IoT, its definition, its history and its inception also highlight the architecture design of IoT that is relied on three dimensions called *"IoT infrastructure";* and the final part in this section discusses the similarities and differences between both IoT and traditional Internet.

2.1. Definitions and History

In 1991, Mark Weiser has described the vision of the future Internet under the name of "*Ubiquitous Computing*". Through this vision he was focused on how to turn on the smart livable environment in the presence of mobile phone technology this provide a powerful multimedia system [6]. Kevin Ashton is a one of the pioneers talk about IoT [2]. According to Atzori A.lera et al [7], classified IoT to three paradigms namely, i) internet oriented (Middleware), ii) things oriented (Sensors), and iii) semantic oriented (Knowledge). In 1999 Neil Gershenfeld was speaking about similar things from the Massachusetts Institute of Technology, MIT Media Lab in his book "*When Things Start to think*".

In 1999 Auto- ID labs and MIT sought to develop Electronic Product Code EPC, and use RFID to identify things on the network. In 2003-2004 the emergence of projects serving IoT idea such as Cooltown, Internet0, and the Disappearing Computer initiative, also IoT start to appear in book titles for the first time. RFID is deployed was published on a massive scale by the US Department of Defense. In 2005 IoT entered a new level when published its first report by International Telecommunication Union ITU. In 2008 a group of companies such as Cisco, Intel, SAP and over 50 other members of companies met to create IPSO Alliance, to promote the use of Internet protocol (IP) and to activate IoT concept. In 2008-2009 IoT was "Born" by Cisco Cisco Internet Business Solutions Group (IBSG) [8]. From the previous perspectives can be defined IoT as a set of smart things/objects such as home devices, mobile, laptop, etc., addressed by a unique addressing scheme and connected to the Internet through a unified framework this framework may be cloud computing. Fig 1 depicts IoT technology.

Fig 1: Internet of Things (IoT) technology

2.2 Architecture and Design

The best design of the architecture is a foundation stone to build a privileged IoT system; this architecture helped to address a lot of issues in the IoT environment such as scalability, routing, networking, etc.. Typically, the IoT architecture approach based on three main dimensions are: *i) Information items*: it includes all items connected to IoT environment may be sensing items, identifying items and control items; *ii) Independent network:* which includes several features such as self-configuration, self-protection, self-adaptation, and self-optimization; and *iii) Intelligent applications:* which have intelligent behavior over the Internet generally; the intelligent behavior may be intelligent control, exchange data methods through network items, data processing, all the applications which are related to the IoT can be classified according to these dimensions [9]. The intersection between these dimensions creates a

new space named "*infrastructure of IoT*", which provides support systems to serve the special things, which can provide various services such as goods identification, location identification and data protection. Fig 2 depicts the three dimensions of IoT and relationship between them.

In this end, There are several approaches to build an architecture of IoT, the paper will focusing on two kinds namely, architecture called "*EPC global network*" and another called "*Unite and ubiquitous IoTs or U2IoTs*", to create an application on IoT, the architectural approach favored which based on an open architecture the EPC global network. The system designed by AutoID center for conveying the dynamic information about objects/things to provide a history of the product movement for the authorized users, the RFID technology plays a key role to differentiate between these mobile objects, this system is called "the EPC global network". The IoT uses the EPC global network as a principle to design the architecture framework [10].

The future architecture of IoT seeks to achieve connection between real-world, cyber-world and social world. Unite and ubiquitous IoTs or U2IoTs is considered as a different kind of IoT architecture, it's used to integrate the physical world with the cyber world. The U2IoTs consists of a set of heterogeneous systems, including unit of IoT to resemble human neural network that provides solutions to specific applications; U2IoTs includes the industrial IoT, local youth, national IoT, and global IoT which integration of multiple Unit IoTs with ubiquitous features, and it is similar to the social organization framework. The main characteristics of U2IoT model are cyber, physical, social co-existence, connectivity and interactivity, space-time consistency and multi-identity status [10].

2.3 Differences between IoT and Traditional network

In the beginning, the IoT technology has broken a lot of the traditional ideas of network and started a new era of telecommunication technology. Can be considered IoT as an extension and expansion network based on the Internet; but it is different from either traditional network or the so-called Internet of people and WSN although considered as backbone to build any IoT block.

The major equation to represent the IoT environment is *"IoT environment= Internet + WSN"*, it is a common statement that uses to express the IoT environment. To analyze and judge the correctness of this statement, must be determined the similarities and differences between IoT, Internet, and WSN according to table 1.

From the previous knowledge about the IoT environment can be judged on this view, it's a wrong; because there are two basic reasons for rejecting this view. First; IoT may not necessarily use IP in all cases for addressing things, because nature of IoT needs lightweight communication protocols, the complexity of the TCP/IP protocol is not suitable in particular, when works with the smart little things. Second, the IoT environment is mainly based on the connected smart objects unlike traditional network. That's what makes them move from only a mere extension of the Internet, also the behavior of IoT depends on the creation of the interoperable systems [10], based on these arguments, can be corrected the previous statement:

IoT= Internet + WSN+ Smart Items surrounded by Intelligent environment.

Finally, IoT supports a set of useful features such as interoperability, self- configuration, self- adaptive and self-protection. The intelligent environment is a way to ensure the existence of a minimum level of the previously mentioned elements within the network.
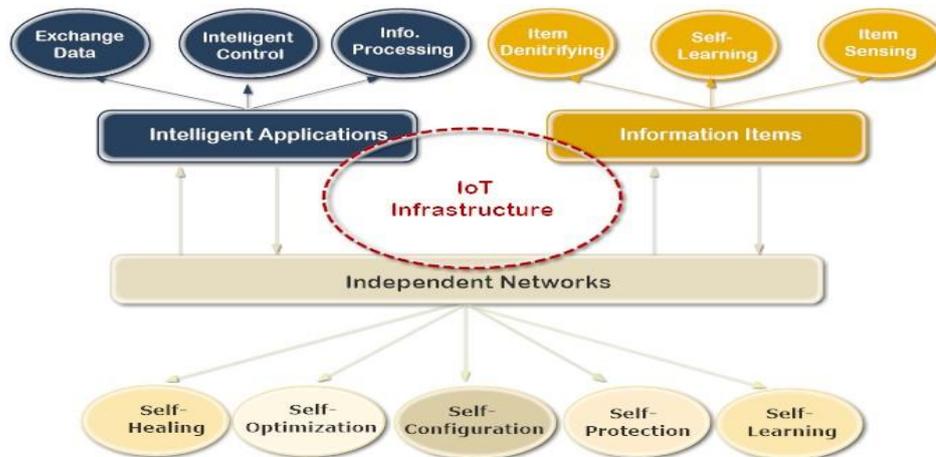

Fig 2: The three Dimensions of IoT

Table 1. The similarities and differences between IoT, Internet, and WSN [10]

Characteristics	IoT	Internet	WSN
Comm. Protocol	Lightweight Comm. protocols.	(TCP/IP)	Lightweight Comm. protocols.
Scale degree of Area	Cover wide area	Cover wide area	Cover local area
Networking Approach	Determine backbone	Determine backbone	Self-organization
Identify objects	Must	Can not	Can
Type of nodes	Active and passive	Active	Active
Network design	WSN+ dynamic smart things+ Internet surrounded by intelligent environment	Set of networks contains set of Fixed objects	Dynamic smart objects
Behavior	Dynamically	Fixed	Dynamically
Networking Time	Timing synchronization	Unlimited	Unlimited

3. CHALLENGES AND RECENT RESEARCH DIRECTIONS

In this section, the paper discusses the bulk of popular challenges or general challenges of the IoT environment; it also displays the recent research directions for each topic. Finally, Table 3 reviews the recent research directions and the proposed solutions for each one of them, in addition to table 4 which reviews the summary for the future research topics in the IoT.

3.1 Networking

Generally, the Networking issue has a great relevance in the Internet because of it includes some of the important factors which uses to manage networks. First of all, traffic and protocols that have a significant impact on the behavior of the network, these points are mentioned in [11] D. Giusto et al. Sought to deal with networking challenges via mobile Ad-Hoc Network. The authors have used mobile ad hoc

networks (MANET) interconnected to fixed networks by different gateway. In IoT, can't be predicted where the object moved, and the object may be needed to transmit from network to another. The biggest problem is in dynamic gateways change and the difficulty of Identifying the location of things. The MANET consists of a number of self-organized mobile nodes or objects and it considered as a way to maintain a connection, additionally Multi-homed ad-hoc is seen as an extension to the existing infrastructure in IoT.

3.2 Routing

Routing process means selecting the best path between the source and the destination to complete the communication process successfully. There are various ways to determine the best path based on the communication protocol type such as a number of hops, costs, and bandwidth. Can be classified routing protocols into two main categories are: i) Reactive protocols: the path is established after

transmission request is made, ii) Proactive protocols: initial path before the request is made. In [12], Sudip Misra et al. proposed the protocol under the name of "fault-tolerant routing protocol" for IoT. This protocol has designed by using learning automate (LA) and cross-layer concept. LA dealing with optimization problems to choose optimal solutions, the need to cross-layer is saving energy of the items of IoT (i.e. FRID).

3.3 Heterogeneity

The IoT environment is the best-known example to represent the heterogeneity issue because it contains a plethora of the different devices in their nature; the main objective of IoT is creating a common way to abstract the heterogeneity of these devices and achieving the optimal exploitation of their functionality. In this vein, the researchers always seek to find an effective method to deal with these devices regardless of their nature.In [13], C. G. Garcia et al. sought to introduce solutions to some of the IoT problems such as interconnection, heterogeneity, and generate an application that allows people to interconnect services over the Internet, these solutions are represented in: creating a domain specific language (DSL), graphic editor and IoT platform Midgar software. For instance, over recent years emerged a lot of applications used to solve the heterogeneous objects problem over the Internet e.g. WhatsApp, Skype and so on, it's considered as a simple example to overcome this problem. The authors have reviewed Midgar software to handle the heterogeneous smart things through the IoT environment and DSL software is designed for the specific purpose, the main idea of this software is generating a domain which allows the interaction between things easy, regardless their nature.

The authors have reviewed Midgar software to handle the heterogeneous smart things through the IoT environment and DSL software is designed for the specific purpose is generating a domain to enable the interaction between things easily regardless their nature. The Midgar Software used to avoid the complexities in traditional methods that are used to handle this problem. In the future the connectivity is won't be limited to the electronic devices, but it will also include people this is will climb the problem; for this reason can be considered Midgar as a first step in this point.Moreover, IoT like any networks uses the service oriented architecture (SOA) approach to enhance the heterogeneous resource behavior (i.e. Sensors and Actuators) and it provides the highest level of flexibility and scalability to the system in both the external integration processes and the exchange processes within the middleware.

3.3.1. *Middleware Layer*

The middleware layer is a software layer or a set of sub-layers interposed between the technological and the application layer, it provides a standard way for representation and communication. In general, the middleware layer supports the transparency concept that is used to hide all complex details from end user; actually the transparency concept is a one of the most distinctive features of distributed systems.The Service oriented Architecture (SOA) is a common example of the middleware technology that is used to deal with IoT, SOA allows to re-use and utilize real world service in a dynamic way [7]. The SOA supports some of the services and one of them is called "Service Level Agreement (SLA)", which used to make an agreement between the service provider and service user, the most important feature of SLA is the

contracted to delivery time service, this feature provides QoS.

The middleware layer consists of three main layers are: *i) Service composition layer:* the common layer on top of SOA middleware; it provides the functionality for composition of single service and builds specific application. This layer concerned about services or providing services only. Service composition architecture consists of individual architecture of the participating services, this architecture published SLA [14].

ii) Service Management layer: the layer allows management in IoT. Service management can be classified into two areas are: i) runtime: services that based on time as a critical factor to implement them directly. ii) Design time: services a part of maintenance lifestyle and service development [15]. Service management layer encompasses is a set of services such as object dynamic discovery, status monitoring, service policy enforcement, service Meta model updates and service configuration, some of middleware include additional features that are related to Qos management and lock management. It's notable that through the service management layer can develop new services during run-time [7].

iii) Object abstraction: the need to object abstraction layer is summarized in vast and heterogeneous objects which scattered through IoT, layer organized harmonizing access to different devices with common language and procedure. Object abstraction includes wrapping layer consists of two sub-layers, interface sub-layer that management, incoming/outcoming messages and it provides an interface exposing the available method through a standard web service interface. Second sub-layer is a communication sub-layer that implements logic at web service methods and translate these methods at devices to communicate with real-world objects [7].

3.4. Interoperability

Interoperability concept can be defined as the ability to create systems or devices cooperating with each other in an efficient way. In [16] Jussi et al. sought to use the semantic level interoperability architecture for pervasive the computing and IoT; the architecture is relied on the semantic information sharing solutions called "smart-M3".

The principle idea of the proposed architecture relies on dividing IoT environment into small spaces to facilitate their management process. A Semantic Information Broker SIB is used to provide methods for agents to share semantic information with each other and also provides monitoring and updating of the physical world in real time. The main observation of the architecture, performance after using the agent interaction operations scale very well also enable interaction with the physical world in real time. The architecture needs for tools the support development and deployment of devices and applications in the future IoT systems.

3.5. Quality of Service (QoS)

Ideally, QoS is defined as "the amount of time that is taken to deliver the message from the sender and the receiver" if this time is equal or less than pre-specified time requirement the QoS is achieved. ITU re-defined QoS concept as a degree of conformance of delivering service to the user by the provider with agreement between them [17]. For QoS assurance, must cope with service models to determine which degree of QoS for each Internet service.

Moreover, Internet services can be classified according to Internet service models which considered as a supplement to provide the following: firstly, the ability to categorize Internet applications by priority; and secondly, determining QoS demands necessary to achieve user satisfaction. A service models consist of three main models based on three factors, namely, a delay factor is concerned with time, which can be classified into Hard Real Time (HRT), Soft Real Time (SRT), and Non-Real Time (NRT), a critical factor is concerned with the kind of process/application (i.e. Sensitive application or not) (yes/no), and finally, an interactivity factor depending on the user's subscription (yes/no). According to table 2, the major types of Internet service models are: an open service model, an Supple service model, and a complete service model, the main function of these categories helping to offer QoS provisioning upon Internet services [18]In [19], Ming ZHOU et al. sought to find an efficient algorithm more suitable with large-scale and real time in IoT, they made a comparison between the three common algorithms are: Integrated Linear Programming (ILP), Genetic Algorithm (GA), and Backtracking Algorithm (BA) to find a suitable algorithm that can deal with this context by efficiently. The authors chose BA as a more suitable algorithm to serve this idea because it's a suitable to cover the large- scale area in IoT and gave the good results in real-time compared with the counterpart of algorithms.

Table 2. Internet Services models

IoT Models	Delay	Process/App.	Interactivity
Open service	Not real time	Not mission critical	Interactive
Supple service	Soft real time	Mission critical	Application dependent
Complete service	SRT/HRT is depending on app.	Mission critical	Not interactive

3.6. Scalability
Scalability is one of the most important challenges of IoT, which means how to deal with the sustainable growth of the Internet in an efficient manner. In the other words, "Scalability is the ability of a system or network to handle the growing scale of any environment without an effect on performance". Currently, the Internet comprises around 9 billion devices with a next era of the Internet which known Web 0.3 or ubiquitous computing it is expected to reach 24 billion devices, the increasing of this number have a broad impact on the performance of the network.

In [5], J. Gubbi et al. sought to apply the cloud computing technology represented in Aneka software with IoT environment. Generally, cloud computing provides a set of features such as high storage resources, scalability, visualization platform and client delivery; plus the cost of each service based on pay-per-use. Aneka cloud computing software provides a utilize storage and computing resources of both public and private cloud.

3.7. Virtualization
Virtualization is known as the ability to share hardware resources among multiple operating systems. The virtualization technology allows for the multiple operating systems and software like applications or services to run upon the same server through creating more than virtual machine inside the physical machine. The vision of this concept helps to increase the performance of the network via increasing utilization, maximizing scalability, saving cost, etc. [20]. Actually, there are three areas used to represent the virtualization technology, namely, i) network virtualization, storage virtualization, and server virtualization.

In [3], S. Alam et al. have created the framework called "an IoT Virtualization Framework based on Sensor as a service notion" this frame consists of three layers are: real world layer, semantic layer and virtualization layer in addition separately database to record useful information. Primarily, the main challenges in the IoT environment can be determined into three items namely, i) there is no registry mechanism, the framework possesses database to overcome this challenge; ii) the heterogeneity and discovery, the proposed framework sought to overcome of this issue through the semantic approach to deal with the heterogeneity by providing a standard language called Sensor Model Language "SensorML"; and finally iii) the interaction between event and service in the IoT environment are absent, the framework uses the Virtualization layer to deal with this challenge by efficient way. The future directions of this framework divided into two points are: enhancing its performance in real-time domain and improving micro-formats for advertising on social networks.

3.8 Big Data
Big Data is a new expression to describe massive data whether structure or unstructured, which is difficult to deal with traditional database methods and software techniques. Simply, Big Data defined as a large volume of data [21]. Dataset considered as a Big Data when it meets 4 V's- value, volume, velocity, and variety. Big Data attracts almost a new industrial field such as online social networks (Twitter, Facebook, and Instagram); the collection of data through the social network is very huge, for example twitter in 2010 producing up 120 terabytes of data of the day [22]. IoT is considered as a good example of Big Data as the amount of data which was collected from deploying sensors through IoT environment was very large and heterogeneous. The coupling between IoT and Big Data was very strong [23].

In [22], Chang Liu et al. sought to introduce a software architecture addressed real-life based on the extraction from the SMARTCAMPUS project, this architecture supported the concept of Big Data into the IoT environment to deal with data collected from sensors. This class of architecture tackled some of challenges such as data storage, avoiding processed bottlenecks and high throughput.

3.9 Cloud Computing
Cloud Computing and IoT are the most popular example to represent the ubiquitous computing field; but IoT is not popular like Cloud Computing, both use the distributed computing concept. Cloud computing is a way to access large amount of computational resources and supports a large number of users in a reliable and decentralized manner; it's also provide software cheaply. Cloud Computing consists of the three main layers are: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Service as a Service (SaaS) each one provide significant features through the cloud data center. Cloud

computing is considered as a standard framework to represent IoT, and both IoT and cloud computing possess a set of benefits and restrictions. IoT represents real world and small things, but it is limited storage in addition to traditional problems in the network such as scalability and privacy; in other side, cloud computing has virtually unlimited capabilities and processing power [24]. The integration of cloud computing with IoT became a very important point of recent researches; to produce system able to overcome the many challenges such as scalability, storage resource and virtualization; can be considered the main objective of this integration is to leverage from cloud computing in processing power which need for sensors and other things [25].

Recently, a lot of researches are mentioned integration between cloud computing concept and IoT; for example not as a limitation in [24], Alessio et al. sought to review the existing integration between IoT and cloud computing in the CloudIoT paradigm and illustrates the benefits from them. First of all, the transparence which come with the virtualization technology to hide the complexity of sensors from the end user; in addition to some of other features such as the storage resources, the cloud computing concept provides high capability to store large amount of data which collected from sensors; the big data considered as a new vision to restructure huge volumes of data through the IoT environment; the computational resources, one of the issues of IoT is limited processing resources Cloud Computing overcome this problem to improve scalability.

The cloud computing also provides a lot of efficient solutions for the most issues of IoT and sought to offer the new visions for these issues such as providing ubiquitous access to sensor data through Sensing-as-a Service (SaaS); enabling automatic control logics implemented in the cloud computing through Sensing and Actuation-as-a-Service (SAaaS); dispatches messaging services triggered by sensor events through Sensor Event-as-a-Service (SEaaS); enabling ubiquitous management of remote sensors through Sensor-as-a-Service (SenaaS); enabling ubiquitous database management through DataBase-as-a-Service (DBaaS); providing ubiquitous access to any kind of data through Data-as-a-Service(DaaS); providing ubiquitous layer-2 connectivity to remote devices through Ethernet-as-a-Service(EaaS); enabling ubiquitous access to policy and identity management functionalities through Identity and Policy Management-as-a-Service(IPMaaS); providing ubiquitous access to recorded video and implementing complex analyses in the Cloud through Video Surveillance-as-a-Service (VSaaS).

3.10 Power Consumption
The power consumption issue is a critical point in wireless networks. Typically, the efficiency of the work of sensors depends on the lifetime of the battery. Nowadays the most of devices are equipped with sensors such as smart mobile phone, tablet and laptop to deal with the modern applications. For instance, the application of weather prediction that is relied mainly on GPS to determine location; once the GPS application is turned on during the whole sensing procedure the battery may be drained very quickly.

In [26], K. Batool et al. have dealt with the power consumption issue by using sniffer agents. The paper was autonomously presented on mobile energy consumption of networked consumer devices to determine the approximation of the current power requirement. The paper

represented the model of the proposed self-organized power consumption approximation (SOPCA) algorithm. The principle idea of this algorithm is the use of wireless connectivity between peer devices and servers, the devices discover other devices to propagate energy sniffer agent (ESA).

ESA locates devices and keeps estimating energy consumption. Source node also locates the other node by using GPS, ESA updates their internal variables based on the observation of local energy consumption then it moves to another node. The mechanism of SOPCA algorithm avoids a re-routing between devices by using flags on the individual devices. The authors used agent-based model (ABM) to test the proposed algorithm over random network.

3.11 Security and privacy
The security rule aims to protect it from threats; these threats classify into two kinds are: the external threats such as attacks on system form attackers and the internal threats represented in misuse of the system or information. There are three main factors of security are: data confidentiality, privacy and truth. Data confidentiality guarantees only the authorized users to access and modify data, and it includes two aspects: first, access control mechanism and second, an object authentication process [27]. Truth is guaranteed to apply security rules into system and common example of truth is digital certificates. Privacy is defined as a control access to personal data; and it allows keeping certain information and data confidential; the features of privacy are secrecy, anonymity and solitude [28]. The most current researches seek to increase and develop privacy in the applications, the Privacy Enhancing Technologies (PET) can be oriented to the subject, the object, the transaction or the system; it is used to protect identity over the Internet [28]. In the IoT environment the security and the privacy are important to guarantee a reliable interaction between the physical world and the cyber world [28].

In [29], Biplob R. Ray et al. proposed a framework dependent on group approach and collaborative approach called "a hybrid approach", and used security check handoff (SCH) with RFID. The SCH is a bet flags (0,1) (on/off) help to keep track of the security state of the tag; also the SCH allows the tag to take a shortcut to clear the security check or re-clearance tag. Notable, the most of the existing protocols which deal with RFID suffer from threats and vulnerabilities such as insecure, inefficient identification, throughput and inadaptability. The proposed protocol provides customization to ensure the adaptability of the new efficient techniques. The development of RFID security protocol makes the IoT more robust distributed structure.

4. THE HOT TOPICS AND RELATED CHALLENGES
The IoT consists of a host of other elements, which are considered as an extension for the general challenges of IoT or it can be called "unique challenges". The section seeks to explain some of these elements in a nutshell.

4.1 Radio frequency Identification (RFID)
RFID is a breakthrough in embedded communication and WSN, RFID is used to generate a unique ID for the object in WSN. It consists of two parts are: passive RFID: which used to power of the reader's interrogation signal to communicate the ID to the RFID, and access control

application as well. Active RFID: readers have their own battery supply and instantiate the communication. RFID uses Ultrawide Bandwidth (UWB) technology to enhance RFID performance in a specific IoT application field. UWB is a technology allows the next generation of RFID to overcome many of the current restrictions in current RFID such as low security, reduce area, and sensitivity to interferences. The RFID contains three key elements are: the RFID tag or transponder that carries object, the RFID tags reader or transceivers that read and write tags and back-end database.

4.2 Wireless Sensor Networks (WSN)

WSN is an important part of IoT, it's considered as a core to build the IoT block, it consists of a group of specialized sensor data are shared among sensor nodes with communication infrastructure for monitoring some of events or states of objects such as temperature, sound, pressure, etc. these sensor nodes work autonomously and can be linked between them by self-organizing. Notable, WSN support the distribution concept between sensor nodes, and each sensor network includes some of elements such as radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source [30]. The section seek to show the components that make up WSN in the following:

- WSN hardware contains a sensor interface, processing units, transceiver units and power supply.

- WSN communication stack the nodes deployed in an ad-hoc manner for most applications.

- WSN middleware is mechanism to combine cyber infrastructure with service oriented architecture (SOA). SOA is an architectural style that enables the composition of applications by using loosely coupled and interoperable services.

- Secure data aggregation; it is a very important to ensure reliable data collected from sensors.

4.3 Addressing Schemas and Communication Protocols

The Internet contains a large amount of objects which needing to determine their location to complete the communication process in an efficient manner, it's considered as a main objective of addressing process. Generally, Internet Protocol (IP) used to identify objects through the Internet; there are two versions of IP, namely, i) IPv4, which uses 32-bit addresses (2^{32} addresses) to identify hosts or objects through the Internet, this process considered as limited to some extent; and ii) IPv6 is the latest version of the Internet protocols uses 128-bit (2^{128} addresses), It covers a large area more than IPv4 [31]. The RFID technology is a way to identify things into WSN and IoT, it generates unique ID to identify the smart objects. Also "IPv6 over Low-power wireless Personal Area Network (6LoWPAN)" IEFT group aims to make IPv6 compatible with low capacity devices.

5. APPLICATIONS

Recently, the IoT technology has appeared as a one of the basics in our lives because it touches a lot of the important sides such healthcare, smart water, transportations, surveillance and so on. Moreover, there are many applications which have emerged to serve this concept.

According to [5] can be divided the IoT applications into four categories can be summarized in the following: i) Personal and home uses WiFi as a backbone providing higher bandwidth data transfer as well as higher sampling rate, the healthcare sector is considered as the most popular example of this category, ii) Enterprise, the information in this category may be collected from the networks, the environment monitoring such as video surveillance is a first common example of this category followed by smart home and smart environment generally, iii) Mobile, the sensor information can be obtained from large scale WSN for online monitoring of travel time the popular example of this category is transportation; lastly, iv) Utilities, the information can be obtained from networks to achieve service optimization and power consumption,Typically, the main target of companies which are using this type of applications is reducing cost and maximizing profit. The best example of this kind is smart grid, smart metering and smart water and quality of drinking water. This section will be reviewed the most popular examples of each type of these mentioned categories earlier, also table 5 summarizes the categories of the IoT applications.

Healthcare: the IoTCloud paradigm [33] has been widely used in the healthcare sector to diagnosis, treatment and tracking the status of the patients remotely. The paradigm must serve four pivots namely, i) tracking: is a function aimed to identify the patient in motion, ii) identification and authentication: identification aimed to reduce mistakes in diagnosis and authentication used to meet with security requirements, iii) data collection: usually aims to reduce processing time and it is related to integrating RFID technology with other health information, lastly iv) sensing: used to provide real time information about the patient [32]. The issues in this area are defined as: control, security, heterogeneity, interoperability and streaming QoS.

Smart environment (i.e. Smart city, smart home): The key idea to gain the smart environment such as smart city or smart home while maintaining the level of service without degradation has relied on the integration between both IoT and cloud computing; over recent year's escalation of attention toward this integration. Generally, The IoT suffers from a host of the thorniest issues, first of all, heterogeneity of objects; there are many middleware technologies are designed to deal with this type of issues, such as RFID middleware and WSN middleware. On the other hand,the cloud computing provides scalability and hide complexity of sensors from end users by using the virtualization technology. The most popular challenges in this type of application are limited to security and real-time applications.Video surveillance: is an intelligent video to monitor the object behavior and activities, it has become an important tool of security-related application and it can be considered as an alternative to self-contained management systems, and the complex video analytics requires Cloud-based solutions, and it can be used to satisfy the need to increase volume of storage capacity of media [32].

Automotive and smart mobility: the aim of this function concentrated on the improvement of transportation and transport through increasing safety road, reducing congestion, and control traffic. Can be considered the integration between Cloud Computing and IoT as a promising opportunity to find effective solution is characterized by high performance, security and lowest cost. The challenges in this type are: identification, heterogeneity of sensors, scalability and dynamic behavior of objects.

Smart energy and smart grid: the biggest problem in the sensors world is power consumption, the battery in sensors may drain very quickly, and both the IoT and Cloud Computing provide intelligent solutions to manage energy distribution and consumption in heterogeneous environments.

6. CONCLUSIONS AND FUTURE DIRECTIONS

IoT is a one the main techniques that is used to express the ubiquitous computing approach, but it still not popular like the cloud computing technology. This paper has sought to highlight the IoT concept in general through the three sections namely; section I, reviewed an overview about the IoT concept via highlighting its history and its inception since 1999 at the hand of Kevin Ashton who considered as one of the pioneers who talked about IoT and even Cisco company now. Then it has reviewed the main idea to design the IoT structure that relies on the integration between three dimensions are: information items, independent network and intelligent applications. Accordingly, the future of the IoT structure relies on the integration among real or physical worlds, cyber-world and social world. Lastly, in this section is pointed out to the differences between both IoT and the traditional network.Section II, reviewed the main general challenges which had a significant impact on the performance of IoT such as communication, networking, Qos, scalability, virtualization, big data, heterogeneity and security; this section sought to illustrate and provide the recent solutions for each element of these challenges. Also, this section reviewed another kind of challenges that are called "unique challenges" under subtitle "The Hot Topics and Related Challenges"

which includes more related challenges to the IoT environment.Finally, section III, reviewed a set of the popular applications which are offered by IoT and the IoTcloud paradigm such as healthcare, smart city, smart grid, smart transportations, etc.. Based on the above, can be considered the IoT environment as a rich search point, and flourishing area to the research in particular in the integration topic with cloud computing, which provides the new sceneries to handle the smart services and applications.

Table 3. Summary for the recent research directions of IoT

Research area	Techniques	Solutions	Open area
Networking [11]	MANET	The authors have used the MANET as a way to maintain connection between things.	• Improving Ad-Hoc network. • Network technologies. • RFID. • Communication protocols.
Routing [12]	Learning automates (LA) & Cross-layer.	The authors proposed a protocol called "fault-tolerant routing" protocol to serve the IoT environment.	• Improving the proposed algorithm to cover the wide range of the application domains
Heterogeneity [13]	Midgar Software	The authors have been sought to improve the interaction between objects or things via the graphic editor that generates model defined by a Domain Specific Language.	• Domain Specific language and graphic editor to generate smart objects. • Insertion of boxes in the graphic editor with support for data analysis and fuzzy logic. • Scalability of IoT platform. • Security and privacy.
Interoperability [16]	Semantic Interoperability Architecture	The authors have been sought to build the semantic interoperability architecture to access the information easily, also the paper used the monitoring and updating events of physical world in real time.	• The architecture needs tools that support development and deployment of devices and applications into the future IoT systems.
QoS [19]	BT, IP & GA	The authors have been reviewed comparison between three algorithms to determine Qos metrics for composes service. BT algorithm is the most appropriate to IoT environment more than ILP & GA, because it suitable to serve both high scale of service and real-time application.	• Decreasing steps of BT algorithm for calculating QoS.
Scalability [5]	Aneka Hybrid cloud computing (private cloud + public cloud)	The authors have used cloud computing technology with IoT environment to improve scalability and provide storage resources.	• Cloud computing. • Energy efficient sensing. • Architecture of IoT. • Data mining. • Secure reprogrammable networks and privacy.
Virtualization [3]	IoT Virtualization Framework based on SenaaS technology.	The authors have created a new framework based on SenaaS notion named it "IoT Virtualization Framework", the main objective of this frame is reusability of the sensor information via web browser.	• The development of IoT framework services micro-formats for advertising on social networks. • Improving the performance of an IoT framework at real time.
Big Data [22]	SMARTCAMPUS.	The authors have sought to improve the software architecture named "real-life" based on extracted from the SMARTCAMPUS project to handle Big	• Cloud Computing. • Scalability/elasticity. • Computation time. • Security.

		Data in the IoT environment.	
Cloud Computing [24]	CloudIoT Paradigm.	The authors have highlighted the integration between the cloud computing and IoT, also reviewed the previous literatures about them.	• Standardization of framework. • Power consuming. • Fog Cloud. • Complex data mining.
Power Consumption [26]	Self-Organized Power Consumption Approximation (SOPCA) Algorithm	The authors have used a self-organizing for dynamic approximation of power consumption to create (SOPCA) algorithm. Also the authors have used Agent-based model to test this algorithm.	• The SOPCA can be further explored by the evaluation of flooding as well as by using artificial intelligence algorithms.
Security [29]	SCH	The authors have used SCH to improve and ensure security of RFID system.	• Improving and addressing the integration of a tag tamper resistance mechanism.

Table 4. Summary for The future research topics in the IoT.

Research Directions	Info.	Open directions
Discovery / identification.	The ability to create a standard addressing schemes more efficient and reliable, additionally, it must be provided convergence of IP and RFID.	• Mapping digital & real. • Device discovery. • Semantic search. • Universal authentications mechanism.
Design / architecture	The IoT architecture uses an open architecture approach to maximize interoperability and handle the heterogeneity.	• Cloud computing. • Ad-Hoc networks. • Adaptive and context-aware architecture.
Networking	The Networking issue includes both routing and communication protocols. it seeks to improve the performance of network through congestion management and traffic.	• Ad-Hoc networks, Hyper networking. • Self-configuration. • Virtualization technology (location transparency). • Self-organization networks.
Standardization	The aim of standardization issue is the ability to create a standard interface or standard framework to achieve highest level of interoperability between devices.	• IoT standardization. • Cloud computing. • Semantic web. • Semantic interoperability.
Energy Consumption	Typically, the efficient of sensors rely on the lifetime of battery. Recently, the micro power technology used to address this issue.	• Semantic interoperability. • Micro battery technologies. • Energy harvesting.
Security	The aim of security is protecting data from unauthorized users. Generally, the security issue contains three levels are: confidentiality, trust, integrity	• Security for cloud computing. • Security for semantic web. • Improving encryption methods. • Privacy policies and trust.

Table 5. The categories of IoT applications

Categories	Services	Connectivity	Challenges
Personal/Home	healthcare	WiFi, 3G, 4GLTE	• Heterogeneity. • Interoperability. • Control methods. • Real-time. • Security. • QoS.
Enterprise	Smart Cities	WiFi, 3G, 4GLTE, Satellite	• Scalability. • Identification and discovery. • Heterogeneity. • Virtualization. • Control methods. • Real-time. • Big data. • Power consumption. • Security.
	Smart Environment	WiFi, 3G, 4GLTE, Satellite	
	Video Surveillance	WiFi, Satellite	

Mobile	Smart Transportation / Smart traffic	WSN, Satellite	• Identification and discovery. • Control methods. • Scalability. • WSN • IoT architecture and design. • Real-time. • Cost.
Utilities	Smart Grid Smart Energy Smart Water	WiFi, Satellite & Celular	• Power consumption. • Scheduling (Load balance). • Real-time. • Scalability. • Control methods. • Cost.

7. REFERENCES

[1] InternetofThings,2014http://www.itu.int/en/publications/gs/pages/publications.aspx?parent=SPOLIR.IT2005&media=paper#

[2] InternetofThings,2015http://www.rfidjournal.com/articles/view?4986.

[3] Sarfraz Alam, Mohammad M. R. Chowdhury, Josef Noll, 2010 SenaaS:An Event-driven Sensor Virtualization Approach for Internet of Things Cloud, Networked Embedded Systems for Enterprise Applications (NESEA), 2010 IEEE International Conference on, 1-6.

[4] Andras Kalmar, Rolland Vida, Markosz Maliosz, 2013 Context-aware Addressing in the Internet of Things using Bloom Filters, Cog l nfoCom 2013· 4th IEEE I nternational Conference on Cognitive I nfocommun ications' (Dec. 2013) 487 - 492.

[5] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, Marimuthu Palaniswami, 2013 Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. Future Generation Computer Systems, 1645-1660.

[6] Daoliang Li, Yingyi Chen, Oct. 2010, Computer and Computing Technologies in Agriculture. Springer, 24-31.

[7] L. Atzori, A. lera, G. Morabito, The Internet of Things: Survey. Computer networks, 2787–2805.

[8] Internet of Things, 2014 http://postscapes.com/internet-of-things-history.

[9] Huansheng Ning, Hong Liu, 2012 Cyber-Physical-Social Based Security Architecture for Future Internet of Things, Advances in Internet of Things, 1-7.

[10] Nihong Wang, Wenjing Wu, 2012 The Architecture Analysis of Internet of Things, Computer and Computing Technologies in Agriculture V IFIP Advances in Information and Communication Technology, 193-198.

[11] D.Giusto, A.lera, G.Morabito, L.Atzori (Eds.), 2010 Objects Communication Behavior on Multihomed Hybrid Ad Hoc Networks, Springer, 3-11.

[12] Sudip Misra, P. Venkata Krishna, Harshit Agarwal, Anshima Gupta, Mohammed S.Obaidat, 2012 An Adaptive Learning Approach for Fault-Tolerant Routing in Internet of Things. IEEE Wireless Communications and Networking Conference: PHY and Fundamentals, 815 – 819.

[13] Cristian González García, B. Cristina Pelayo G-Bustelo, Jordán Pascual Espada, Guillermo Cueva-Fernandez, 2014. Midgar: Generation of heterogeneous objects interconnecting applications.DomainSpecificLanguageproposal for Intern etof Things scenarios", Computer Networks, 143-158.

[14] SOA, 2014 http://en.wikipedia.org/wiki/Service-oriented_architecture.

[15] Gopala Krishna Behara, Srikanth Inaganti. 2007 Approach to Service Management In SOA Space, BPTrends.

[16] Jussi Kiljander, Alfredo D'elia , Francesco Morandi , Pasi Hyttila, Janne Takalo-Mattila , Arto Ylisaukko-Oja , Juha-Pekka Soininen, Tullio Salmon Cinotti. 2014 Semantic Interoperability Architecture for Pervasive Computing and Internet of Things, 856 – 873.

[17] ITU-T E.860. Framework of a service level agreement 2002,2014.https://www.itu.int/ITUD/tech/events/2005/Nairobi2005/Presentations/Day2/Nairobi_2_2_4.pdf.

[18] Marie-AurelieNef, Leonidas Perlepes, Sophia Karagiorgou, George I.Stamoulis, Panayotis K.Kikiras, 2012 Enabling QoS in the Internet of Things, CTRQ: The Fifth International Conference on Communication Theory, Reliability, and Quality of Service, 33-38.

[19] Ming ZHOU, Yan MA, 2013 QoS-aware computational method for IoT composite service, The Journal of China Universities of Posts and Telecommunications, 35-39.

[20] Lenn-Wei Lin, Chien-Hung Chen, Chi-YiLin, 2013 Integrating QoS awareness with virtualization in cloud computing system for delay-sensitive application, Future Generation Computer Systems, 478–487.

[21] Bigdata,2014http://www.webopedia.com/TERM/B/big_data.html.

[22] Chang Liu, Chi Yang, Xuyun Zhang, Jinjun Chen, 2014 External Integrity Verification for OutSourced Big Data in Cloud and IoT: A Big Picture, Future Generation Computer System.

[23] Cyril Cecchinel, Matthieu Jimenez, Sebastien Mosser, Michel Riveill, 2014 An Architecture to Support the Collection of Big Data in the Internet of Things, Services (SERVICES), 2014 IEEE World Congress on, 442-449.

[24] Alessio Botta, Walter de Donato, Valerio Persico, Antonio Pescape, 2014 On the Integration of Cloud Computing and Internet of Things, 2014 International Conference on Future Internet of Things and Cloud (FiCloud), 23 – 30.

[25] Noura Alhakbani, Mohammed Mehedi Hassan, M. Anwar Hossain, and Mohammed Alnuem, 2014 A Framework of Adaptive Interaction Support in Cloud-Based Internet of Things (IoT) Environment, G.Fortino et al. (Eds.): IDCS 2014, LNCS 8729, 136-146.

[26] [26] Komal Batool, Muaz A. Niazi, 2015 Self-Orgnized Power Consumption Approximation in the Internet of Things, 2015 IEEE International Conference on Consumer Electronics (ICCE).

[27] Rolf H. Weber, Romana Weber, 2010 Internet of Things, Springer, 41-68.

[28] Huansheng Ning, 2013 Unit and Ubiquitous Internet of Things, CRC Press.

[29] Biplob R. Ray, Jemal Abawajy, Morshed Chowdhury, 2014 Scalable RFID security framework and protocol supporting Internet of Things , Computer Networks, 89-103.

[30] Wirelesssensornetwork,2014http://en.wikipedia.org/wiki/ Wireless_sensor_network.

[31] IP address, 2014 http://en.wikipedia.org/wiki/IP_address.

[32] Xiang Sheng, Jian Tang , Xuejie Xiao ,Guoliang Xue, 2013 Sensing as a Service: Challenges, Solutions and Future Directions, IEEE Sensors Journal, 3733 – 3741.

[33] OpenSourceIoTCloud,2015https://www.sites.google.com /site/opensourceiotcloud/installation-guide,.