ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 3, pp: (218-228), Month: July - September 2016, Available at: www.researchpublish.com

A Survey on The Internet of Things: Technologies, Architecture, Applications and Challenges

[1]Almuthanna A. Alageel, [2]Linah M. Alhazzaa

[1]Computer Research Institute, King Abdulaziz City for Science and Technology, Riyadh, Saudi Arabia
[2]Department of Computer Science, Princesses Nora bint Abdulrahman University, Riyadh, Saudi Arabia

Abstract: **With the advanced research in Wireless Sensor Networks (WSN), Radio-Frequency Identification (RFID) and other enabling technologies, Internet of Things (IoT) becomes a promising service to most kind of users. In this paper, the definition of the IoT is introduced with tracing back where it is come from. In addition, it covers a brief description of the current enabling technologies that support the infrastructure of the IoT. Moreover, the current architecture of the IoT is explained with two proposed architecture that exploit Cloud Computing to enhance the scalability and flexibility. Furthermore, health care and medicine, transportation and equipment maintenance applications have been discussed and how they could enhance to each industry. This paper ends the body of the topic by identifying the challenges and future work of the IoT i.e. issues related to security, privacy, self-management capabilities, power consumption, heterogeneity issues, scalability, naming and identification and communication connectivity are all covered.**

Keywords: **Internet of Things; Wireless Sensor Networks; Ubiquitous Computing; Pervasive Computing; RFID; Security.**

I. INTRODUCTION

With the different innovations, such as enhancing the Internet infrastructure, the availability and reliability of RFID, sensor networks and embedded systems, the term of Internet of Things (IoT) has been initially proposed in 1999 by Kevin Anshton [1]. The IoT considered as a new paradigm that connects the pervasive objects, which may be attached with a sensor, actuator, RIFD...etc., to each other. With the abundant addresses that IPv6 could offer, these objects have a unique address [2]. To clarify the ambiguity of the IoT as a term, the two words describe the elements that constitute IoT i.e. “Internet” means everything is connected to network and “things” means all objects. The purpose of the IoT is to facilitate the exchange information among different objects -in securely manner- that connected to the Internet and to provide the ability for making decision automatically and manually [3].

The IoT would not be applicable without the enabling technologies, such as sensing and communication technologies as well as middleware. In this survey, we describe the IoT concept in section 2 followed by the enabling technologies in section 3, we also covered the current and proposed architectures in section 4, applications that benefits from the IoT in section 5 and challenges and issues of IoT in section 6.

II. INTERNET OF THINGS CONCEPT

The Internet of Things concept (IoT) is wide. As a result, there are several definitions of IoT because it has been studied from different perspectives. Therefore, in this paper, various definitions of IoT from diverse perspectives will be covered.

IoT defines as a collection of various technologies, such as RFID and barcode that provide the ability of a huge number of things to communicate with each other by using diverse networking technologies in order to form an enormous and intelligent network [1].

Internet of Things can be defined from three perspectives i.e. things, Internet and semantic. From things viewpoint, the primary concentration of IoT is to combine common objects into a unified framework. As defined by "Cluster of European research projects on the Internet of Things", things refer to participants who are active by communicating and exchanging information either among themselves or with the environment and able to perform operations independently with or without human intervention when any event occurs [6]. From Internet perspective, according to IP for Smart Objects (IPSO) Alliance, Internet Protocol (IP) is a network technology connecting enormous number of smart communication devices. This makes IP a key player in making IoT real [4]. The semantic perspective focuses on how to manage the exchange of data among smart devices [7] because the number of devices that are connected to the Internet dramatically is increasing. Therefore, standardization of resource descriptions is necessary in order to achieve interoperability of heterogeneous resources. The general notion is to separately store the semantic meanings of objects from the data [7]. It is clear that semantic-oriented and things-oriented and internet-oriented paradigms can contribute in realization the Internet of Things. The benefit of IoT is clear through convergence these three visions as shown in Fig.1 [4]. According to [8], Internet of Things helps in interconnection of different sensing devices to transfer data across different platforms by using a unified framework to support sophisticated applications. This requires data to be sensed, analyzed and represented with using Cloud computing as the unified framework [8].

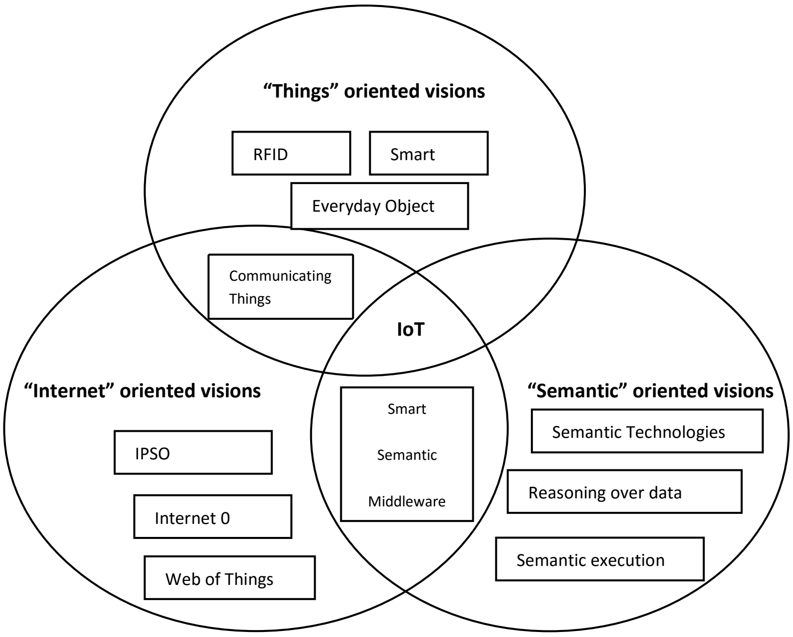

Fig.1 The intersection of diverse visions leads to "Internet of Things" paradigm [4]

III. ENABLING TECHNOLOGIES

There are several technologies, today, that enable IoT, for instance, radio-frequency Identification (RFID), wireless sensor networks (WSN) and ZigBee network, global positioning system (GPS), barcode and data storage and analytics. There are other technologies that can be helpful to IoT, such as biometrics, machine vision and actuators.

A. Radio-Frequency Identification (RFID)

RFID plays a major role in IoT, where each object may be attached with RFID tags. This is mainly to allow IoT to track each object by RIFD reader, which does not require detecting signal in a line of sight. Reader can detect the signal by the attached antenna that radiates signals to RIFD tags and then receives it from the RIFD tags. As regards to RIFD tags, it may be active, passive or semi-active. It consists of microchips, antenna and battery. While for these passive tags, battery is not applicable [9]. These tags can store up to 2KB which means it works like an assistant to the whole system and not meant to process heavily data.

A major concern regarding to RIFD is reducing the cost. The major component that influences the overall cost of RIFD is the type of data storage and the range of communication [9]. Read-only data storage type considered being the cheapest with limited uses while read-write may provide dynamic several functionalities that could be changed any time with high cost. The moderate cost of data storage is write-once-read-many that may be suitable for wide range of applications [9]. The other cost factor is the communication range. Active and semi-active RIFD tags can work for longer range unlike passive RIFD tags. The former could be applicable on average range of 70 meters with higher price while the latter is designed to be in a range of 6 meters which is definitely cheaper. In IoT, the researchers tend to deploy passive large number of RIFD tags in each object more than those of active or semi active tags [9].

B. Barcode

The main technologies that are used for identification are Two-dimensional bar code and RFID. Using bar code technology is popular in warehousing and industrial control [10]. An identification number of an object can be coded using a one-dimensional or two-dimensional barcodes. The label that has the barcode can be either attached to or printed on the object. The cost of this technology is low especially in case of printing the label directly to the object. On the other hand, using barcodes for identification has some disadvantages. It is not possible to identify more than one item at a time, which increases the manual task to identify objects with barcodes [11]. One disadvantage of one- dimensional barcode can store small data size, which makes limited expression for numbers and characters. Therefore, two-dimensional bar codes were developed [10].

RFID has several advantages in compared to barcodes. Using RFID makes things communicate to each other without human interference. The ability to change is another advantage of RFID. That means it is possible to reuse RFID tags. More information can be stored in RFID tags. However, RFID has disadvantages. The disadvantage of RFID is RFIDs readers are more expensive to setup and to maintain while barcodes are cheap in compared to RFID tags [12]. As a result, it is clear that using RFID is favored rather than barcodes because of its several brilliant advantages in compared to barcodes, but it would be better if the cost of RFID becomes lower.

C. Wireless Sensor Networks (WSN)

Wireless sensor networks (WSN) are distributed autonomous sensors that deploy for several applications, such as monitoring temperatures, objects, vehicles …etc. These sensors are called nodes that composed of a power source, transceiver, microcontroller and transducer. WSN offers a short range of communication among nodes that act as a router [9]. Eventually, these nodes are communicating with the gateways to pass their data to the Internet, hence, benefiting Internet of Things. The most wireless sensor products are based on the IEEE 802.15.4, which operate at low bit rate in wireless personal area network with low-power [13] [14]. However, another promising sensor networks for Internet of Things is ZigBee networks, which is non-standard protocol [15].

RFID can increase the capability of sensor networks because it can provide the sensible feature to insensible object. However, wireless sensor networks have several benefits in compared to conventional RFID. One advantage is the ability of sensors to sense more information in comparison with RFID technology, such as environmental conditions like pressure and temperature and others [16]. On the other hand, wireless sensor networks have some disadvantages. The speed of wireless sensor network is lower and they have some security issues.

D. ZigBee Networks

ZigBee network is a high-level communication protocol based on IEEE 802.15 that designed to be applied in 10-100 meters of range line-of-site with lower power consumption [17]. These features can benefit the application of IoT as applying ZigBee can be at lower cost, longer battery life with acceptable range for wide range of applications.

ZigBee consists of four devices i.e. ZigBee Coordinator (ZC), which works as ZigBee network roots responsible to start the network as well as to provide security keys, ZigBee Routers (ZR), that extend the range of networks, ZigBee End Device (ZED), which performs a specific control job or sensing, then talks to the parent node whether either ZC or ZR [18] [9]. In Fig. 2, ZigBee Network Topology for a smart home is illustrated.

There are several protocols can be used. Zigbee, Z-Wave technologies are not based on the Internet Protocol (IP). Zigbee was designed by the ZigBee Alliance. The purpose of designing Zigbee is for low-rate applications. The ZigBee consists of four layers i.e. physical, medium access control, network, and application. The first two layers are based on IEEE 802.15.4 standard while the remaining layers are based on the ZigBee specification. Zigbee also has several functionalities, such as security. The roles of device that are defined by Zigbee include coordinator, router and end device. Another wireless network technology is Z-Wave that is also not based on IP [9]. It is evolved by ZenSys and supported by the Z-Wave Alliance [18]. It is used for the reliability of transmission of short messages between control unit and different numbers of nodes in the network [9]. This protocol is composed of several layers i.e. physical, MAC, transfer, routing and application. Two kinds of devices are defined by Z-Wave i.e. controllers and slaves [19]. LoWPANs (Low-Power Wireless Personal Area Networks) are another wireless network technology but is based on IP, which means can be linked to other IP based networks by using edge routers. 6LoWPAN has diverse kinds of devices [19].

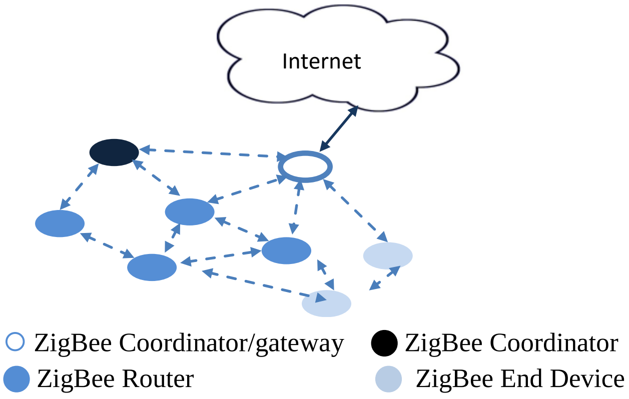

Fig.2 ZigBee Network Topology [18]

E. Data Storage and Analytics

As the amount of data is growing exponentially, data storage and its management have become extremely critical. Using data centers provides several benefits, such as efficiency energy use and high reliability. Storing and using the data should be done in an intelligent way for intelligent monitoring. Therefore, developing centralized or distributed artificial intelligence algorithms is necessary to smartly store and use data for sensing. In addition, there is a need to develop a centralized infrastructure in order to enhance storage and analytics. Since 2012, one solution is the cloud storage that has become more commonly used in addition to the possibility of cloud based analytics and visualization platforms in the few coming years [8]. Because using IoT leads to collecting massive amounts of information, it is recommended to use the cloud storage if it provides security and prevents data leakage.

F. Visualization

Visualization is one of the key needs of any IoT application. It provides an efficient communication of the user with the environment. Using touch screen makes smart devices easier to use. Creating visualization that can be easily understood is necessary to make a person effectively take advantage of the IoT revolution. Using 3D screens instead of 2D provides meaningful and significant information for users. The whole idea of visualization is to bring out a meaningful and easy to understand information from a raw data [8]. Therefore, using visualization plays an important role in assisting to make IoT applications widely used.

G. Addressing and Naming Methods

Addressing methods are important in making IoT successful. Appropriate address schemes will help in identification of every device in a unique manner and also in controlling every remote device via Internet. Some of the parameters that need to be kept in mind while designing an addressing scheme include persistence, uniqueness, reliability, and scalability. The URN (Uniform Resource Name) system is essential in developing IoT. In a URN system, each device that is accessible via the URL will be replicated [8]. As a consequence, developing novel addressing schemes is very significant and required to make IoT more reliable, which helps in deployment of IoT.

IV. ARCHITECTURE

The IoT architecture has been described in several papers. M. Wu et al. described the most architecture that received more agreement [3]. In this section, the three-layer architecture and other proposed architecture are described.

A. Current Architecture

The current architecture of the IoT includes three-layers i.e. perception, network and application layers shown in Fig.3 which is illustrated from technical point of view [3].

The Perception Layer is the interface to physical world that includes several enabling technologies such as RFID, WSN, ZigBee networks, camera, GPS and actuators. Gathering information and identifying the objects are the main functions of this layer [3]. In Network Layer, data are transmitted after being received from the perception layer. Therefore, it is expected to perform operations, such as network management, information management and processing data [3]. The upmost layer is the Application Layer where the users and industry requirements are met intellectually [3] by exploiting and integrating the available perceptional technologies that are connected by the Internet. In addition, the Application Layer provides the Human-Computer Interface to present data in efficient way to the end users.

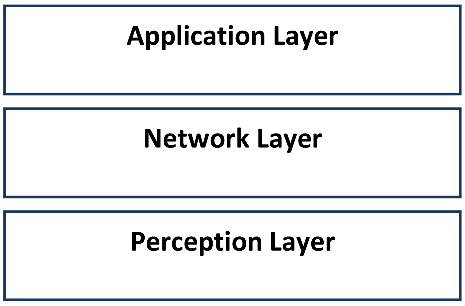

Fig. 3 3-layer architecture of the IoT [3]

B. A new Architecture

The researchers in [3] criticize the current architecture as it lacks from providing a business and management model. Therefore, the authors propose a new architecture that divides the IoT into five layers as shown in Fig. 4. The perception layer works similar to that one of the current architecture that has been described earlier. The data are passed to the Transport layer where the packets are routed to its destination. This layer provides several protocols, such as IPv6 to give a unique address for each object. In addition, the main techniques that are available in Transport layer are FFTx, Wifi, Zigbee, Infrared, 3G, and Bluetooth …etc [3].

Next, the packet is processed in the Processing Layer such that information of objects that is received from the Transport Layer are stored, analyzed and processed. The authors extract this layer due to large amount of objects collects mass-data; therefore, it may needs to use some techniques, such as intelligent processing, database and primarily Cloud Computing (CC) [3]. This layer is the brain of the new architecture where huge amount of data is available to be analyzed and processed through several techniques; therefore, the IoT can take the advantages of advancing research on other area, such as Cloud Computing or Machine Learning.

However, the layered approach may include some redundant functionalities among layers, which may increase the overhead. The processed data are passed to the Application Layer where diverse applications are developed, for example, smart transportation, location-based service [3], health care or smart homes. This layer is dynamic and can meet the users or industry requirement. The uppermost layer of the new architecture is the Business Layer where the business and profit model can be applicable [3]. It also acts as the manager of the entire system where requests are sent.

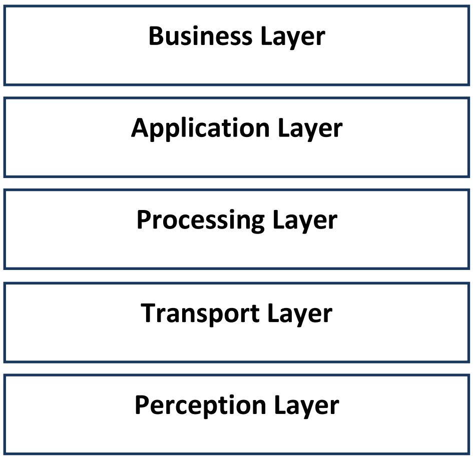

Fig. 4 A new architecture proposed by [3]

C. Internet-Centric Approach

In [3], the author proposed another approach called Internet-Centric which connects the IoT to Cloud Computing as a backbone. Internet-Centric could provide flexibility of estimating costs in logical manner as well as does provide highly-scalability [3]. This approach can integrate many vendors together to act as one Internet of Things without paying the extra cost of such services that are not needed. Sensing providers can ask for more storage from Cloud storage, then provide the information to another service provider through Cloud itself [3]. It can also allow developers to develop an analytic tool or Artificial Intelligence experts to develop a tool for machine learning or data mining as well as computer graphics specialist to provide a wide range of visualization tools [3]. This approach is open to developer's ideas, hence, enhancing the performance and the available tools for the IoT users. The architecture of the Internet-Centric approach is illustrated in Fig.5.

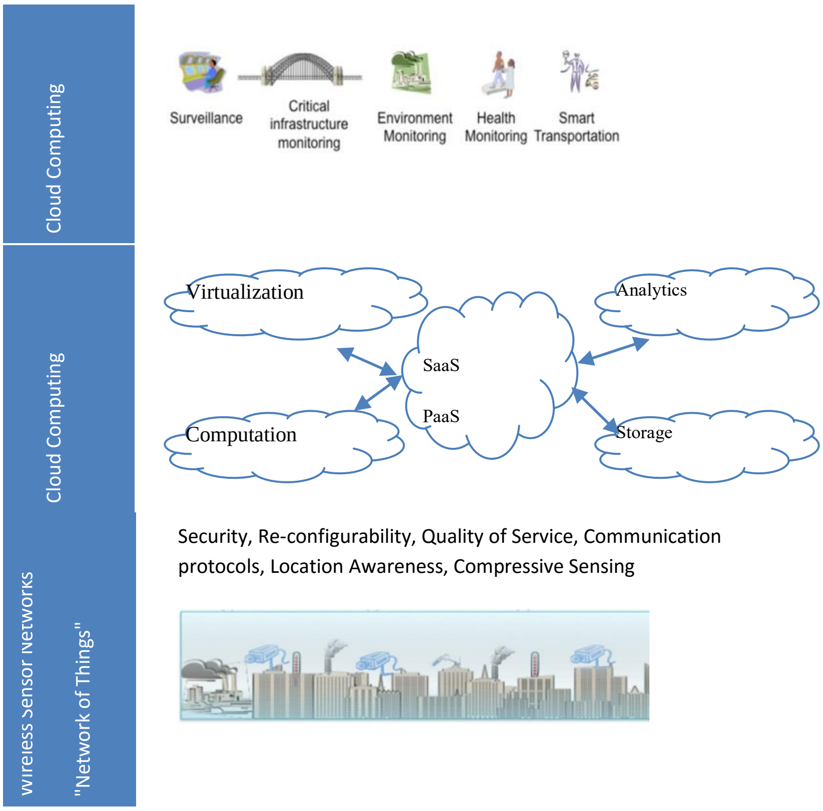

Fig.5 Internet-Centric Approach [3]

V. APPLICATIONS

With the flexibility and scalability of the Internet of Things, a wide range of applications can be offered. For example, transportation, logistics, healthcare and medicine, smart environment, personal domain, geography, agriculture and smart grid. In this section, seven applications will be discussed i.e. health care and medicine, smart homes, predication of natural hazard applications, equipment maintenance, agricultural and breeding applications, transportation and supply chain management and smart supermarket.

A. Health Care and Medicine

There are plenty of applications that have been suggested to service health care and medicine domain. That includes medical equipment, medication control and medical information management.

In [20], F. Hu et al. suggest using the IoT to monitor the process of production and delivery and to trace medical equipment for safety issues. With RFID tags, readers who are responsible for production line could easily identify the medication information, then to be transferred to the database. This can be carried out through the whole process of medication production, circulation and use. Therefore, the medication quality can be maintained until the storage or delivery stage. In case of identifying a quality problem, tracing back the damaged medicine can be easily handled via the medicine name, category storage, origin and sales.

Another aspect is that, RFID tags for unique IDs can guarantee the anti-counterfeit of medical equipment and medication due to the availability of accessing public database that includes each medicine or medical equipment decryption, manufacturer, unique ID … etc. This could help hospitals or even patients to easily manage verification if the medicine or medical equipment is counterfeited or not. Information includes also the medical refuse information system in order to trace back the refused medicine with cooperative database among different hospitals and transportation firms [20].

In addition, medical information management can be enhanced with the IoT. When patient comes to the hospital, all patient history can be accessed. Therefore, reducing the incidents of giving a wrong drug or even avoiding the mismatching of the infant identification after the patient giving a birth [21].

B. Smart Homes

The Internet of Things can make our surrounding environment intelligent, which makes our lives more convenient and safe. The definition of smart home is a house that has the technology in order to control both home appliances and systems in an automatic way [22]. Designing smart homes has become feasible because of available IoT technologies, which provides several advantages. As a result of designing smart homes, it is possible to manage the power consumption, to help locating things in an easier way, to maintain home safety and to interact with different devices [23]. It is obvious that smart homes assist in control different appliances, such as television, which reduce the power consumption and enhance the efficient energy use. For Instance, the lighting will be turned off if there is no one in the room. In addition, they help in the security or safety of homes because the security system can prevent any stranger from entering a house and this system may be connected to the police department or the fire detection system that can reduce the possibility of the outbreak of fires.

C. Prediction of Natural Hazard Applications

An application can be used to predict the natural and hazardous disasters, such as earthquakes and tornadoes using several types of sensors to sense the different environmental conditions. That helps to take suitable actions earlier. In addition, the IoT can assist to determine the lacking of water at diverse locations, such as catchment area. Collection of sensors is used to monitor the water level and to alert user of any hazardous disaster, such as flooding or leak of sewage into the river [23]. As a result, using these types of application will play a role on reducing the number of injuries and death resulting of natural disasters.

D. Transportation

All kind of transportation such as cars, trains and bicycles as well as the infrastructure itself can be equipped with sensors and actuators. Infrastructure sensors can pass the information related to the traffic status and can help driver to choose better route, visitors to be guided inside the city and monitor the transported goods [24].

By providing abundant information of the road status, driver can navigate the route more dynamically, helping the driver to avoid busy traffic especially in rush hour, so it can save her time and can increase the productivity of community. In terms of good transportation, monitoring the traffic could help the delivery department to track their goods and the driver's status i.e. launch time, delivery time, break time and the chosen route [24]. In addition, collision detection and avoidance systems can be established, which benefits both governmental authorities and drivers [24]. This also could help the parties who are involved in the car incident to resolve their issues regarding who is compensating whom and what percentage by looking up to the record information.

E. Equipment Maintenance

In [25], the authors propose an intelligent equipment maintenance using the Internet of things called (IITEM). The Intelligent Internet of things for equipment maintenance (IITEM) can observe the information of electrical and mechanical equipment dynamically and statically. IITEM came to solve the safety issues of the equipment that can influence resources and daily production to avoid catastrophic accidents, hence, reducing or avoiding causalities and equipment damages [25].

IITEM can provide important functionalities and information, such as a safety operation system that can monitor the dynamic operating parameters of the most important equipment's, to feedback the users with real-time analysis of operating status and being able to predict the failure before occurs in most cases and finally in case of hazard, alarm is launched automatically [25]. In addition, IITEM is able to feedback the system itself for optimal control of the equipment's operating status [25]. IITEM can reduce the number of employees by leaving several functionalities to the automated system that benefits from the Internet of Things.

F. Agricultural and Breeding Applications

A group of different sensors can be used for sensing and processing collected data to notify the farmer about which part of the farm requires special care and attention. The farmer can be informed about diverse conditions, such as drought. This helps in raising and improving the agricultural productivity [23]. In addition, the IoT technology can help to track the movement of agricultural animals [4]. Another benefit is the farmer can avoid money loss as a result of monitoring the land condition. That keeps the harvest in a better condition.

G. Supply Chain Management and Smart Supermarket

The importance of IoT has appeared also in the supply chain management field, such as automation and inventory control. In January 2005, Wal-Mart required suppliers to equip their shipments with RFID tags in order to control the inventory. In addition, there are several IoT applications in the supermarkets. For instance, an application acts as a guide in the supermarket depending on the shopping list that was chosen before [6]. Designing smart supermarkets help blind people to be independent from others for purchasing needs. The blind people use RFID readers when they enter the supermarket. Every shelf has a passive RFID tag in addition to unique ID that gives a description about the class of the product [26]. As a result of using IoT applications, inventory control and other tasks become easier and accurate. It is clear that smart supermarket makes the shopping more convenient and fast.

VI. CHALLENGES AND FUTURE WORK

With ubiquitous existence and availability of the Internet of things, this may bring tremendous risks to people life in terms of security and privacy. If the intruder attacks the system, it may obtain complete information about a person or every single bit in the environment. An intruder, then, can abuse the system and request for more than just collecting information such as shutdown the plant in the industrial applications, or manipulate the patient's data. Therefore, in this section, we give more focus on security and privacy issues. In addition, we covered briefly, self-management capabilities, power consumption, heterogeneity issues, scalability, naming and identification and communication connectivity.

A. Security

The IoT as a system can be attacked physically due to the physically absent of the user most of times. In addition, most enabling technologies for communication are wireless which is more vulnerable to attacker than wired networks. One of the main issue that facing researcher to resolve these problems is that, most IoT component are passive devices that implemented for saving power consumption, hence, it lacks from weak abilities to perform complex security scheme [27].

Moreover, authentication and data integrity are another concerns. Again, a stronger authentication scheme require sophisticated infrastructures and servers to manage identities, which is not applicable for the IoT as it relies on exchanging messages among passive RIFDs tags [27] [28]. As regards to the data integrity, an adversary can manipulate data stored in passive RFID tags or when data are sent through the network [29]. One of proposed solution is called Harbor, which is for protecting data inside memory of both passive RIFD tags and wireless sensor networks. The software is based on fault isolation called sandboxing in order to provide a restriction of memory access and control flow [30]. While Harbor can be used for protection against first attack, Keyed-Hash Message Authentication Code (HMAC) can be used to protect messages against second attack [31]. HMAC is based on sharing keys between two devices and then perform Hash functions [31]. In case of the IoT, the two devices are the passive RFID, for example, and the destination.

B. *Privacy*

The privacy issue is a major challenge for the IoT industry to be involved in every aspect of our life. In several countries of the world where they have many legislation related to privacy, if information is leaked based on technical problem that would cost the IoT vendor not only money but also its reputation to protect people's information. Even people who are not using the IoT services, their privacy may be threaten by tracking objects application. Platform for Privacy Preferences (P3P) [32] allows the users to use a language to describe the policies that may fit into goal of the IoT privacy such as tracking system is gathering data of the position of people unless if neglect their identity, which should be deleted from the storage once it is already used for instant purpose [33].

C. *Self-Management Capabilities*

The unexpected scale of deployment of the IoT need to be paid attention for more efficient of the IoT. Internet success is based on the minimalistic best-effort service approach i.e. programming and management have been considered for scalability [27]. It would support the scalability of the IoT if similar approach is applied due to billions of heterogeneous objects are connected together which support solutions such as context-awareness, self-management, self-organization and self-healing [27].

D. *Power Consumption*

Increasing the power consumption of the network is obvious because of increasing data rates and the number of both connected devices and Internet-based services. That means the network power consumption will be increased dramatically in the future because of IoT. As a result, it is important to utilize green technologies that can make the network devices consume less power as much as possible [23]. However, it is clear that available energy capacity is not suitable for the future requirements [27]. It is obvious that there are several devices that are battery-powered, so it is necessary to develop power management techniques in order to efficient energy use by utilizing less power as possible.

E. *Heterogeneity Issue*

IoT consists of several heterogeneous objects. However, it is difficult to manage heterogeneous applications and devices, which considered as a main challenge of IoT [5]. IoT has to support heterogeneous environment, which means IoT has to be able to combine several heterogeneous kinds of technologies, devices and services. Therefore, the system should support enormous and various types of applications which have different features and requirements, such as bandwidth. In addition, the system should be able to support different devices whose characteristics are different, such as computational power, mobility and storage power. The design of unified framework and communication protocols is a challenge because of supporting heterogeneous technologies, devices and services [27]. As a result, several researches should have been conducted to overcome heterogeneity issues in order to make dealing with heterogeneous environment easier and to guarantee the quality of services.

F. *Scalability*

The scalability is another main challenge in order to accommodate the extreme growth in devices number. Existence of several devices may affect the performance of communications techniques. This issue is clear in wireless context because it is difficult to have coherent and stable view of the topology. As a result, communications protocols cause multiple challenges because of the difficulty of managing the network in a large distributed environment. Devices should have self-managing capabilities. On other word, they can manage themselves without external interference to support the prospective scale of IoT [27]. Because of the IoT, the number of devices is increasing. Therefore, providing the ability to deal with a huge number of devices is required to make IoT more reliable.

G. Naming and Identification

In the IoT, huge number of items will be connected in order to bring several creative and useful services. A unique identity is required for every object over the Internet. Therefore, there is a need for effective naming and identity management techniques that have the ability to dynamically assigning and managing unique identity for enormous count of objects [23]. In addition, there is a necessity to develop different technologies in order to solve identity encoding and identity encryption [4]. Because IoT depends mainly on the ability to effectively identify an object, it is significant to overcome this major challenge in an efficient way, which makes the IoT more reliable.

H. Communication Connectivity

With different enabling technologies for communications, issues of energy consumption, compatibility, and antenna design have to be addressed. In addition, system with tremendous connections is hard to manage, therefore it should identify who needs to be connected in order to provide the communication abilities that able to avoid problems such as excessive interference [27].

VII. CONCLUSION

The Internet of Things can change the way we live by relying on the computer systems in everywhere, not just limited by using personal computer or smartphone. Human will never be connected to a technology or innovation in most their life as much as the IoT since the innovation of the electricity. In this paper, we give a definition and concept of the IoT followed by some necessary technologies that enable the IoT to be ready to use. However, the IoT is still in its infancy i.e. even its architecture is in a debate situation as I showed earlier three different architectures.

The IoT can be useful for every aspect of our life. In this paper, we explained how seven different sector can enhance their services through the IoT. In addition, we discus three different architecture model for the IoT in current time and future. Finally, the research trend of the IoT is mainly about security and privacy in the first place. Other issues such as self-management capabilities that has to be provided to support scalability is mentioned briefly. The interoperability of different communication technologies could causes a considerable overhead.

REFERENCES

[1] Y. Liu and G. Zhou, "Key technologies and applications of internet of things. In Intelligent Computation Technology and Automation (ICICTA), 2012 Fifth International Conference on," in Intelligent Computation Technology and Automation (ICICTA), 2012 Fifth International Conference on, IEEE, 2012.

[2] J. Höller, V. Tsiatsis, C. Mulligan, S. Karnouskos, S. Avesand, D. Boyle, From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence., Elsevier, 2014.

[3] M. Wu, T. Lu, F. Ling, J. Sun, and H. Du, "Research on the architecture of Internet of things," in Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on, IEEE, 2010.

[4] D. Bandyopadhyay and J. Sen, , "Internet of Things: Applications and Challenges in Technology and Standardization," Wireless Personal Communications, vol. vol. 58, no. no. 1, pp. pp. 49-69, 2011.

[5] E. Welbourne, L. Battle, G. Cole, K. Gould, K. Rector, S. Raymer, M. Balazinska, G. Borriello, "Building the Internet of Things Using RFID," IEEE Internet Com-puting, vol. vol.13, no. no.3, p. pp. 48–55, May–June 2009.

[6] H. Sundmaeker, P. Guillemin, P. Friess and S. Woelfflé, "Vision and challenges for realising the Internet of Things C," in luster of European Research Projects on the Internet of Things (CERP IoT), 2010.

[7] C. C. Aggarwal, "The Internet of Things: A Survey from the Data-Centric Per-spective," in Managing and Mining Sensor Data New York: Springer, vol. ch. 12, pp. pp. 383-428, 2013.

[8] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Generation Computer Systems, vol. 7, no. 29, pp. 1645-1660, 2013.

[9] K. Hwang, J. Dongarra, and GC. Fox, Distributed and cloud computing: from parallel processing to the internet of things, Morgan Kaufmann, 2013.

[10] H. Xuechen, "The two-dimensional bar code application in book management," in in Web Information Systems and Mining (WISM), Sanya, 2010.

[11] L. W. F. Chaves and Z. Nochta, " Breakthrough Towards the Internet of Things: Building Scalable and Global RFID Networks," in in Unique Radio Innovation for the 21st Century, Heidelberg, 2010.

[12] D. Cika, M. Draganic and Z. Sipus, "Active wireless sensor with radio frequency identification chip," in in MIPRO, Opatija, 2012.

[13] "IEEE 802.15 Working Group for WPAN," [Online]. Available: http://ieee802.org/15. [Accessed 15 10 2014].

[14] M. Petrova, J. Riihijarvi, P. Mahonen, and S. Labella, "Performance study of ieee 802.15. 4 using measurements and simulations," in Wireless communications and networking conference, 2006. WCNC 2006. IEEE, 2006.

[15] Y. Xiaolin, J. Zhigang, C. Nanzhong, Z. Wenjun, and W. Zhongning, "The research and implementation of zigbee protocol-based internet of things embedded system," in Inofmration Engineering and Electronic Commerce (IEEC), 2010 2nd International Symposium, IEEE, 2010.

[16] H. Liu, M. Bolic, A. Nayak, and I. Stojmenovie, "ntegration of RFID and wire-less sensor networks ,," in in Sense Worksop at ACN SenSys, Sydney, Australia., 2007.

[17] "ZigBee Specification FAQ," ZigBee Alliance, [Online]. Available: http://www.zigbee.org/Specifications/ZigBee/FAQ.aspx. [Accessed 15 10 2014].

[18] "ZigBee Specification Network Topology," ZigBee Alliance, [Online]. Available: http://www.zigbee.org/Specifications/ZigBee/NetworkTopology.aspx. [Accessed 16 10 2014].

[19] C. Gomez and J. Paradells, "Wireless home automation networks: A survey of architectures and technologies," IEEE Comm. Mag, vol. vol. 48, no. no. 6, p. pp. 92–101, 2010.

[20] F. Hu, D. Xie, and S. Shen, "On the Application of the Internet of Things in the Field of Medical and Health Care," in Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing, IEEE, 2013.

[21] A.M. Vilamovska, E. Hattziandreu, R. Schindler, C. Van Oranje, H. De, "RFID Application in Healthcare – Scoping and Identifying Areas for RFID Deployment in Healthcare Delivery," in RAND Europe, February 2009.

[22] K. Bing, L. Fu, Y. Zhuo and L. Yanlei, "Design of an Internet of Things-based Smart Home System,”," in in Intelligent Control and Information Processing (ICICIP), Harbin, 2011.

[23] R. Khan, S.U. Khan, R. Zaheer S. Khan, "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," in in Frontiers of Infor-mation Technology (FIT), Islamabad, 2012.

[24] S. Haller, S. Karnouskos and C. Schroth, The Internet of Things in an Enterprise Context, Future Internet – FIS 2008, Springer Berlin Heidelberg, 2009, pp. 14-28.

[25] X. Xiaoli, Z. Yunbo, and W. Guoxin, "Design of intelligent Internet of things for equipment maintenance," in Intelligent Computation Technology and Automation (ICICTA), 2011 International Conference on, IEEE, 2011.

[26] M. Mathankumar and T. Kavitha, " Design and Implementation of Smart Super-market System for Vision Impaired," International Journal of Engineering and Technology (IJET), , vol. vol.5, no. no.1, pp. pp. 215-219, 2013.

[27] M. Zorzi, A. Gluhak, S. Lange, and A. Bassi, "From today's intranet of things to a future internet of things: a wireless-and mobility-related view," Wireless Communications, IEEE, vol. 6, no. 17, pp. 44-51, 2010.

[28] R. Aggarwal, and ML. Das, "RFID security in the context of internet of things," in Proceedings of the First International Conference on Security of Internet of Things, ACM, 2012.

[29] T. Karygiannis, B. Eydt, G. Barber, L. Bunn, and T. Phillips, "Guidelines for securing radio frequency identification (RFID) systems," NIST Special publication, no. 80, 2007.

[30] R. Kumar, E. Kohler, and M. Srivastava, "Harbor: software-based memory protection for sensor nodes," in Proceedings of the 6th international conference on Information processing in sensor networks,, ACM, 2007.

[31] H. awczyk, R. Canetti, and M. Bellare., "HMAC: Keyed-hashing for message authentication," IETF, 1997.

[32] L. Cranor, M. Langheinrich, M. Marchiori, M. Presler-Marshall, and J. Reagle, "The platform for privacy preferences," W3C recommendation, 2002.

[33] J. Wickramasuriya, M. Datt, S. Mehrotra, and N. Venkatasubramanian, "Privacy protecting data collection in media spaces," in Proceedings of the 12th annual ACM international conference on Multimedia,, ACM, 2004.