

# Internet of Things (IoT): A Literature Review

Somayya Madakam, R. Ramaswamy, Siddharth Tripathi

IT Applications Group, National Institute of Industrial Engineering (NITIE), Vihar Lake, Mumbai, India  
Email: [somu4smart@gmail.com](mailto:somu4smart@gmail.com), [ramaswamy2008@gmail.com](mailto:ramaswamy2008@gmail.com), [siddharth.iita@gmail.com](mailto:siddharth.iita@gmail.com)

Received January 2015

---

## Abstract

One of the buzzwords in the Information Technology is Internet of Things (IoT). The future is Internet of Things, which will transform the real world objects into intelligent virtual objects. The IoT aims to unify everything in our world under a common infrastructure, giving us not only control of things around us, but also keeping us informed of the state of the things. In Light of this, present study addresses IoT concepts through systematic review of scholarly research papers, corporate white papers, professional discussions with experts and online databases. Moreover this research article focuses on definitions, geneses, basic requirements, characteristics and aliases of Internet of Things. The main objective of this paper is to provide an overview of Internet of Things, architectures, and vital technologies and their usages in our daily life. However, this manuscript will give good comprehension for the new researchers, who want to do research in this field of Internet of Things (Technological GOD) and facilitate knowledge accumulation in efficiently.

## Keywords

Internet of Things, IoT, RFID, IPv6, EPC, Barcode, Wi-Fi, Bluetooth, NFC, ZigBee, Sensors, Actuators

---

## 1. Introduction

“The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it” was Mark Weiser’s central statement in his seminal paper [Weis 91] in Scientific American in 1991. There is a sea change in human’s daily life as well as in working conditions in organizations after the arrival of IT and ITeS technologies. This is becoming well-known concept across many horizontal and vertical markets including a common man’s everyday life in the society, as it has several applications. The development of the Internet of Things [IoT] has been primarily driven by needs of large corporations that stand to benefit greatly from the foresight and predictability afforded by the ability to follow all objects through the commodity chains in which they are embedded [1]. The ability to code and track objects has allowed companies to become more efficient, speed up processes, reduce error, prevent theft, and incorporate complex and flexible organizational systems through IoT [2]. The IoT is a technological revolution that represents the future of computing and communications, and its development depends on dynamic technical innovation in a number of important fields, from wireless sensors to nanotechnology. They are going tag the each object for

identifying, automating, monitoring and controlling.

## 2. Internet of Things

The Internet of Things is a novel paradigm shift in IT arena. The phrase “Internet of Things” which is also shortly well-known as IoT is coined from the two words i.e. the first word is “Internet” and the second word is “Things”. The Internet is a global system of interconnected computer networks that use the standard Internet protocol suite (TCP/IP) to serve billions of users worldwide. It is a network of networks that consists of millions of private, public, academic, business, and government networks, of local to global scope, that are linked by a broad array of electronic, wireless and optical networking technologies [3]. Today more than 100 countries are linked into exchanges of data, news and opinions through Internet. According to Internet World Statistics, as of December 31, 2011 there was an estimated 2, 267, 233, 742 Internet users worldwide (Accessed data dated on 06/06/2013: from the Universal Resource Location <http://www.webopedia.com/TERM/I/Internet.html>). This signifies 32.7% of the world’s total population is using Internet. Even Internet is going into space through Cisco’s Internet Routing in Space (IRIS) program in the coming fourth years (Accessed on 10/05/2012: <http://www.cisco.com/web/strategy/government/space-routing.html>). While coming to the Things that can be any object or person which can be distinguishable by the real world. Everyday objects include not only electronic devices we encounter and use daily and technologically advanced products such as equipment and gadgets, but “things” that we do not do normally think of as electronic at all—such as food, clothing; and furniture; materials, parts and equipment, merchandise and specialized items; landmarks, monuments and works of art and all the miscellany of commerce, culture and sophistication [4]. That means here things can be both living things like person, animals—cow, calf, dog, pigeons, rabbit etc., plants—mango tree, jasmine, banyan and so on and non-living things like chair, fridge, tube light, curtain, plate etc. any home appliances or industry apparatus. So at this point, things are real objects in this physical or material world.

### 2.1. Definitions

There is no unique definition available for Internet of Things that is acceptable by the world community of users. In fact, there are many different groups including academicians, researchers, practitioners, innovators, developers and corporate people that have defined the term, although its initial use has been attributed to Kevin Ashton, an expert on digital innovation. What all of the definitions have in common is the idea that the first version of the Internet was about data created by people, while the next version is about data created by things. The best definition for the Internet of Things would be:

“An open and comprehensive network of intelligent objects that have the capacity to auto-organize, share information, data and resources, reacting and acting in face of situations and changes in the environment”

Internet of Things is maturing and continues to be the latest, most hyped concept in the IT world. Over the last decade the term Internet of Things (IoT) has attracted attention by projecting the vision of a global infrastructure of networked physical objects, enabling anytime, anyplace connectivity for anything and not only for any one [4]. The Internet of Things can also be considered as a global network which allows the communication between human-to-human, human-to-things and things-to-things, which is anything in the world by providing unique identity to each and every object [5]. IoT describes a world where just about anything can be connected and communicates in an intelligent fashion that ever before. Most of us think about “being connected” in terms of electronic devices such as servers, computers, tablets, telephones and smart phones. In what’s called the Internet of Things, sensors and actuators embedded in physical objects—from roadways to pacemakers—are linked through wired and wireless networks, often using the same Internet IP that connects the Internet. These networks churn out huge volumes of data that flow to computers for analysis. When objects can both sense the environment and communicate, they become tools for understanding complexity and responding to it swiftly. What’s revolutionary in all this is that these physical information systems are now beginning to be deployed, and some of them even work largely without human intervention. The “Internet of Things” refers to the coding and networking of everyday objects and things to render them individually machine-readable and traceable on the Internet [6]–[11]. Much existing content in the Internet of Things has been created through coded RFID tags and IP addresses linked into an EPC (Electronic Product Code) network [12].

## 2.2. Genesis

The Internet of Things is a technological revolution that represents the future of computing and communications, and its development depends on dynamic technical innovation in a number of important fields, from wireless sensors to nanotechnology (Accessed dated on 20/04/2013 from URL: <http://www.ieccr.net/comsoc/ijcis/>). The first Internet appliance was a Coke machine at Carnegie Melon University in the early 1980s. Programmers working several floors above the vending machine wrote a server program that chased how long it had been since a storage column in the machine had been unfilled. The programmers could connect to the machine over the Internet, check the status of the machine and determine whether or not there would be a cold drink awaiting them, should they decide to make the trip down to the machine. Though the buzzword “Internet of Things” evolution was set out a way back in 1980’s with coffee vending machine, the original term is coined by Kevin Ashton, the Executive Director of Auto-ID Labs in MIT in 1999. The concept of IoT first became very popular through the Auto-ID centre in 2003 and in related market analysts publications. Right from the beginning the Internet of Things evolution started, there were many things or objects connected to the internet for the different applications through diverse technologies depending on the type of object for the comfort ability of Human.

## 2.3. Time Series

Accessed from the URL dated on 24/3/2013: <http://postscapes.com/internet-of-things-history>.

1999: The term Internet of Things is coined by Kevin Ashton, Executive Director of the Auto-ID Center in Massachute Institute of Technology (MIT)

1999: Neil Gershenfeld first time spoken about IoT principles in his book titled “When Things Start to Think”

1999: MIT Auto-ID Lab, originally founded by Kevin Ashton, David Brock and Sanjay Sarma in this year.

They helped to develop the Electronic Product Code

2000: LG announced its first Internet of refrigerator plans

2002: The Ambient Orb created by David Rose and others in a spin-off from the MIT Media Lab is released into wild with NY Times Magazine naming it as one of the Ideas of Year

(2003-2004): RFID is deployed on a massive scale by the US Department of Defense in their Savi program and Wal-Mart in the commercial world

2005: The UN’s International Telecommunications Union (ITU) published its first report on the Internet of Things topic

2008: Recognition by the EU and the First European IoT conference is held

2008: A group of companies launched the IPSO Alliance to promote the use of IP in networks of “Smart Objects” and to enable the Internet of Things

2008: The FCC voted 5-0 to approve opening the use of the ‘white space’ spectrum

(2008-2009): The IoT was born according to Cisco’s Business Solutions Group

2008: US National Intelligence Council listed the IoT as one of the 6 “Disruptive Civil Technologies” with potential impacts on US interests out to 2025

2010: Chinese Premier Wen Jiabao calls the IoT a key industry for China and has plans to make major investments in Internet of Things

2011: IPv6 public launch-The new protocol allows for 340, 282, 366, 920, 938, 463, 463, 374, 607, 431,768, 211, 456 ( $2^{128}$ ) addresses

## 2.4. Aliases

Different people calling Internet of Things with different names but the objective of IoT is same in the broad sense. The aliases of Internet of Things includes Web of Things, Internet of Objects, Embedded Intelligence, Connected Devices and Technology Omnipotent, Omniscient and Omnipresent. In addition to these, it has also calling as counting (1) Cyber Physical Systems “Integrations of computation and physical processes”, in which bringing the real and virtual worlds together (2) Pervasive Computing is a computer environment in which virtually every object has processing power with wireless or wired connections to a global network (3) Ubiquitous Computing or Calm technology, where technology becomes virtually invisible in our lives (4) Machine-to-Machine Interaction means no human intervention whilst devices are communicating end-to-end (5) Human-Computer Interaction involves the study, planning, and design of interaction between people and computers (6)

Ambient Intelligence is a developing technology that will increasingly make our everyday environment sensitive and responsive.

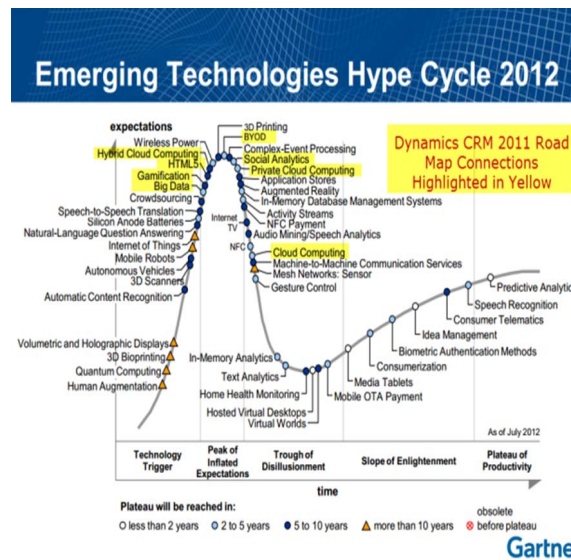
## 2.5. Requirements

For successful implementation of Internet of Things (IoT), the prerequisites are (a) Dynamic resource demand (b) Real time needs (c) Exponential growth of demand (d) Availability of applications (e) Data protection and user privacy (f) Efficient power consumptions of applications (g) Execution of the applications near to end users (h) Access to an open and inter operable cloud system.

According to another author, there are three components, which required for seamless Internet of Things (IoT) computing (a) Hardware—composed of sensors, actuators, IP cameras, CCTV and embedded communication hardware (b) Middleware—on demand storage and computing tools for data analytics with cloud and Big Data Analytics (c) Presentation—easy to understand visualization and interpretation tools that can be designed for the different applications.

## 2.6. Gartner's Hype cycle

Gartner's Information Technology Hype Cycle [13] is a way to represent emergence, adoption, maturity and impact on applications of specific technologies (2) In the adjacent graph, X- axis denotes expectations and Y- axis denotes time factors (3) Internet of Things has been identified as one of the emerging technologies in Internet of Things as noted in Gartner's IT Hype Cycle (4) It has been forecasted that IoT will takes around 5-10 years for market adoption as of the 2012. See the picture for data.



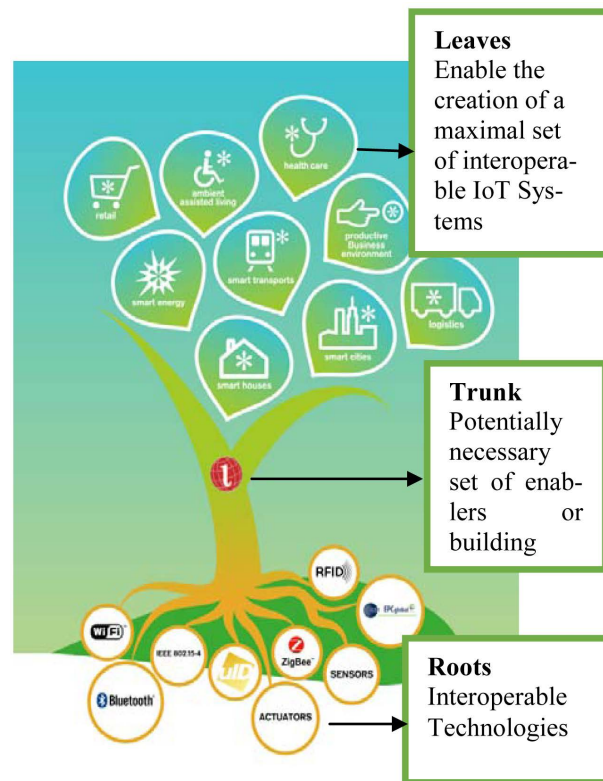
<http://www.wired.com/2012/10/gartner-hype-cycle-2012>

## 3. Architectures

One of the main problems with the IoT is that it is so vast and such a broad concept that there is no proposed, uniform architecture. In order for the idea of IoT to work, it must consist of an assortment of sensor, network, communications and computing technologies, amongst others [14]. Here, some of IoT architectures or models are given by several researchers, authors and practitioners.

### 3.1. European FP7 Research Project

(1) This is to be used as a blueprint for IoT concrete architecture design; (2) Model: Architectural Reference Model (ARM); (3) Developed By: Project partners of the European FP7 Research Project IoT-A; (4) Derived From: Business considerations, application-based requirements and current technologies.



### 3.2. ITU Architecture

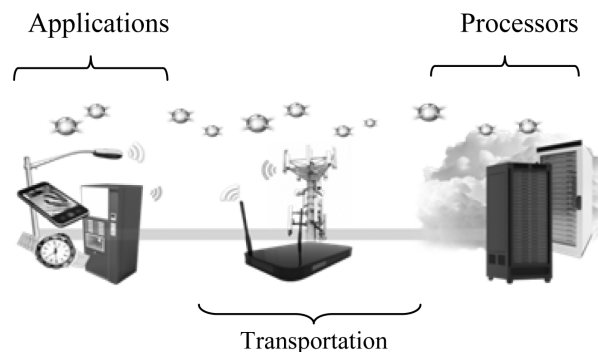
According to the recommendations of the International Telecommunication Union (ITU), the network, Architecture of Internet of Things consists of

- (a) The Sensing Layer
- (b) The Access Layer
- (c) The Network Layer
- (d) The Middleware Layer
- (e) The Application Layers

These are like the Open Systems Interconnection (OSI) reference model in network and data communication.

### 3.3. IoT Forum Architecture

The IoT Forum says that the Internet of Things Architecture is basically categorized into 3 types including Applications, Processors and Transportation.



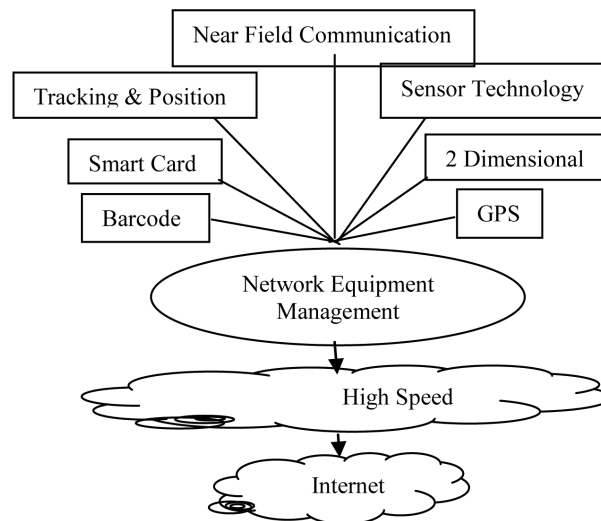
Accessed dated on 2/09/2014 from <http://iotaforum.com/>.

### 3.4. Qian Xiaocong, Zhang Jidong Architecture

According to Qian Xiaocong and Zhang Jidong (2012), the traditional IoT is formed by three layers. The bottom is perception layer, whose function is cognizing and collecting information of objects. The middle is transportation layer which consists of OFC, mobile phone networks, and fixed telephone networks, broadcasting networks, and closed IP data networks for each carrier. And finally the top is application layer, where abundant applications run. Typical applications include in this layer are smart traffic, precise agriculture, intelligent logistics, smart industry, environment protection, mining monitor, remote nursing, safety defense, smart government etc.

### 3.5. Kun Han, Shurong Liu, Dacheng Zhang and Ying Han's (2012)'s Architecture

In “Initially Researches for the Development of SSME under the Background of IoT”, the model is



## 4. Technologies

The Internet of Things [15] was initially inspired by members of the RFID community, who referred to the possibility of discovering information about a tagged object by browsing an internet address or database entry that corresponds to a particular RFID or Near Field Communication [16] technologies. In the research paper “Research and application on the smart home based on component technologies and Internet of Things”, the included key technologies of IoT are RFID, the sensor technology, nano technology and intelligence embedded technology. Among them, RFID is the foundation and networking core of the construction of Internet of Things [17]. The Internet of Things (IoT) enabled users to bring physical objects into the sphere of cyber world. This was made possible by different tagging technologies like NFC, RFID and 2D barcode which allowed physical objects to be identified and referred over the internet [18]. IoT, which is integrated with Sensor Technology and Radio Frequency Technology, is the ubiquitous network based on the omnipresent hardware resources of Internet, is the Internet contents objects together. It is also a new wave of IT industry since the application of computing fields, communication network and global roaming technology had been applied. It involves in addition to sophisticated technologies of computer and communication network outside, still including many new supporting technologies of Internet of Things, such as collecting Information Technology, Remote Communication Technology, Remote Information Transmission Technology, Sea Measures Information Intelligence Analyzes and Controlling Technology etc. [19].

### 4.1. Radio Frequency Identification (RFID)

Radio Frequency Identification (RFID) is a system that transmits the identity of an object or person wirelessly using radio waves in the form of a serial number [20]. First use of RFID device was happened in 2<sup>nd</sup> world war in Brittan and it is used for Identify of Friend or Foe in 1948. Later RFID technology is founded at Auto-ID center in MIT in the year 1999. RFID technology plays an important role in IoT for solving identification issues



of objects around us in a cost effective manner [5]. The technology is classified into three categories based on the method of power supply provision in Tags: Active RFID, Passive RFID and Semi Passive RFID. The main components of RFID are tag, reader, antenna, access controller, software and server. It is more reliable, efficient, secured, inexpensive and accurate. RFID has an extensive range of wireless applications such as distribution, tracing, patient monitoring, military apps etc. [21].

#### 4.2. Internet Protocol (IP)

Internet Protocol (IP) is the primary network protocol used on the Internet, developed in 1970s. IP is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries. The two versions of Internet Protocol (IP) are in use: IPv4 and IPv6. Each version defines an IP address differently. Because of its prevalence, the generic term IP address typically still refers to the addresses defined by IPv4. There are five classes of available IP ranges in IPv4: Class A, Class B, Class C, Class D and Class E, while only A, B, and C are commonly used. The actual protocol provides for 4.3 billion IPv4 addresses while the IPv6 will significantly augment the availability to 85,000 trillion addresses [22]. IPv6 is the 21st century Internet Protocol. This supports around for  $2^{128}$  addresses.

#### 4.3. Electronic Product Code (EPC)

Electronic Product Code (EPC) is a 64 bit or 98 bit code electronically recorded on an RFID tag and intended to design an improvement in the EPC barcode system. EPC code can store information about the type of EPC, unique serial number of product, its specifications, manufacturer information etc. EPC was developed by Auto-ID centre in MIT in 1999. EPCglobal Organisation [Wikipedia, “EPCglobal”, 2010] which is responsible for standardization of Electronic Product Code (EPC) technology, created EPCglobal Network [Wikipedia, “EPCglobal Network”, 2010] for sharing RFID information. It has four components namely Object Naming Service (ONS), EPC Discovery Service (EPCDS), EPC Information Services (EPCIS) and EPC Security Services (EPCSS).

#### 4.4. Barcode

Barcode is just a different way of encoding numbers and letters by using combination of bars and spaces of varying width. Behind Bars [23] serves its original intent to be descriptive but is not critical. In The Bar Code Book, Palmer (1995) acknowledges that there are alternative methods of data entry techniques. Quick Response (QR) Codes the trademark for a type of matrix barcode first designed for the automotive industry in Japan. Bar codes are optical machine-readable labels attached to items that record information related to the item. Recently, the QR Code system has become popular outside the automotive industry due to its fast readability and greater storage capacity compared to standard. There are 3 types of barcodes of Alpha Numeric, Numeric and 2 Dimensional. Barcodes are designed to be machine readable. Usually they are read by laser scanners, they can also be read using a cameras.

#### 4.5. Wireless Fidelity (Wi-Fi)

Wireless Fidelity (Wi-Fi) is a networking technology that allows computers and other devices to communicate over a wireless signal. Vic Hayes has been named as father of Wireless Fidelity. The precursor to Wi-Fi was invented in 1991 by NCR Corporation in Nieuwege in the Netherlands. The first wireless products were brought on the market under the name WaveLAN with speeds of 1 Mbps to 2 Mbps. Today, there are nearly pervasive Wi-Fi that delivers the high speed Wireless Local Area Network (WLAN) connectivity to millions of offices, homes, and public locations such as hotels, cafes, and airports. The integration of Wi-Fi into notebooks, handhelds and Consumer Electronics (CE) devices has accelerated the adoption of Wi-Fi to the point where it is nearly a default in these devices [24]. Technology contains any type of WLAN product support any of the IEEE 802.11 together with dual-band, 802.11a, 802.11b, 802.11g and 802.11n. Nowadays entire cities are becoming Wi-Fi corridors through wireless APs.

#### 4.6. Bluetooth

Bluetooth wireless technology is an inexpensive, short-range radio technology that eliminates the need for pro-

prietary cabling between devices such as notebook PCs, handheld PCs, PDAs, cameras, and printers and effective range of 10 - 100 meters. And generally communicate at less than 1 Mbps and Bluetooth uses specification of IEEE 802.15.1 standard. At first in 1994 Ericson Mobile Communication company started project named "Bluetooth". It is used for creation of Personal Area Networks (PAN). A set of Bluetooth devices sharing a common channel for communication is called Piconet. This Piconet is capable of 2 - 8 devices at a time for data sharing, and that data may be text, picture, video and sound. The Bluetooth Special Interest Group comprises more than 1000 companies with Intel, Cisco, HP, Aruba, Intel, Ericson, IBM, Motorola and Toshiba.

#### 4.7. ZigBee

ZigBee is one of the protocols developed for enhancing the features of wireless sensor networks. ZigBee technology is created by the ZigBee Alliance which is founded in the year 2001. Characteristics of ZigBee are low cost, low data rate, relatively short transmission range, scalability, reliability, flexible protocol design. It is a low power wireless network protocol based on the IEEE 802.15.4 standard [25]. ZigBee has range of around 100 meters and a bandwidth of 250 kbps and the topologies that it works are star, cluster tree and mesh. It is widely used in home automation, digital agriculture, industrial controls, medical monitoring & power systems.

#### 4.8. Near Field Communication (NFC)

Near Field Communication (NFC) is a set of short-range wireless technology at 13.56 MHz, typically requiring a distance of 4 cm. NFC technology makes life easier and more convenient for consumers around the world by making it simpler to make transactions, exchange digital content, and connect electronic devices with a touch. Allows intuitive initialization of wireless networks and NFC is complementary to Bluetooth and 802.11 with their long distance capabilities at a distance circa up to 10 cm. It also works in dirty environment, does not require line of sight, easy and simple connection method. It is first developed by Philips and Sony companies. Data exchange rate now days approximately 424 kbps. Power consumption during data reading in NFC is under 15ma.

#### 4.9. Actuators

An actuator is something that converts energy into motion, which means actuators drive motions into mechanical systems. It takes hydraulic fluid, electric current or some other source of power. Actuators can create a linear motion, rotary motion or oscillatory motion. Cover short distances, typically up to 30 feet and generally communicate at less than 1 Mbps. Actuators typically are used in manufacturing or industrial applications. There are three types of actuators are (1) Electrical: ac and dc motors, stepper motors, solenoids (2) Hydraulic: use hydraulic fluid to actuate motion (3) Pneumatic: use compressed air to actuate motion. All these three types of actuators are very much in use today. Among these, electric actuators are the most commonly used type. Hydraulic and pneumatic systems allow for increased force and torque from smaller motor.

#### 4.10. Wireless Sensor Networks (WSN)

A WSN is a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations (Wikipedia). Formed by hundreds or thousands of motes that communicate with each other and pass data along from one to another. A wireless sensor network is an important element in IoT paradigm. Sensor nodes may not have global ID because of the large amount of overhead and large number of sensors. WSN based on IoT has received remarkable attention in many areas, such as military, homeland security, healthcare, precision agriculture monitoring, manufacturing, habitat monitoring, forest fire and flood detection and so on [26]. Sensors mounted to a patient's body are monitoring the responses to the medication, so that doctors can measure the effects of the medicines [27].

#### 4.11. Artificial Intelligence (AI)

Artificial Intelligence refers to electronic environments that are sensitive and responsive to the presence of people. In an ambient intelligence world, devices work in concert to support people in carrying out their every-



day life activities in easy, natural way using Information and Intelligence that is hidden in the network connected devices. It is characterized by the following systems of characteristics (1) Embedded: Many Networked devices are integrated in to the environment (2) Context Aware: These devices can recognize you and your situational context (3) Personalized: They can be tailored to your needs (4) Adaptive: They can change in response to you (5) Anticipatory: They can anticipate your desires without conscious mediation.

## 5. Conclusions

IoT has been gradually bringing a sea of technological changes in our daily lives, which in turn helps to making our life simpler and more comfortable, though various technologies and applications. There is innumerable usefulness of IoT applications into all the domains including medical, manufacturing, industrial, transportation, education, governance, mining, habitat etc. Though IoT has abundant benefits, there are some flaws in the IoT governance and implementation level. The key observations in the literature are that (1) There is no standard definition in worldwide (2) Universal standardizations are required in architectural level (3) Technologies are varying from vendor-vendor, so needs to be interoperable (4) For better global governance, we need to build standard protocols. Let us hope future better IoT.

## References

- [1] Lianos, M. and Douglas, M. (2000) Dangerization and the End of Deviance: The Institutional Environment. *British Journal of Criminology*, **40**, 261-278. <http://dx.doi.org/10.1093/bjc/40.2.261>
- [2] Ferguson, T. (2002) Have Your Objects Call My Object. *Harvard Business Review*, June, 1-7.
- [3] Nunberg, G. (2012) The Advent of the Internet: 12th April, Courses.
- [4] Kosmatos, E.A., Tselikas, N.D. and Boucouvalas, A.C. (2011) Integrating RFIDs and Smart Objects into a Unified Internet of Things Architecture. *Advances in Internet of Things: Scientific Research*, **1**, 5-12. <http://dx.doi.org/10.4236/ait.2011.11002>
- [5] Aggarwal, R. and Lal Das, M. (2012) RFID Security in the Context of "Internet of Things". *First International Conference on Security of Internet of Things*, Kerala, 17-19 August 2012, 51-56. <http://dx.doi.org/10.1145/2490428.2490435>
- [6] Biddlecombe, E. (2009) UN Predicts "Internet of Things". Retrieved July 6.
- [7] Butler, D. (2020) Computing: Everything, Everywhere. *Nature*, **440**, 402-405. <http://dx.doi.org/10.1038/440402a>
- [8] Dodson, S. (2008) The Net Shapes up to Get Physical. *Guardian*.
- [9] Gershenfeld, N., Krikorian, R. and Cohen, D. (2004) The Internet of Things. *Scientific American*, **291**, 76-81. <http://dx.doi.org/10.1038/scientificamerican1004-76>
- [10] Lombreglia, R. (2010) The Internet of Things, Boston Globe. Retrieved October.
- [11] Reinhardt, A. (2004) A Machine-to-Machine Internet of Things.
- [12] Graham, M. and Haarstad, H. (2011) Transparency and Development: Ethical Consumption through Web 2.0 and the Internet of Things. *Research Article*, **7**.
- [13] Jayavardhana, G., Rajkumar, B., Marusic, S. and Palaniswami, M. (2013) Internet of Things: A Vision, Architectural Elements, and Future Directions. *Future Generation*.
- [14] Gigli, M. and Koo, S. (2011) Internet of Things, Services and Applications Categorization. *Advances in Internet of Things*, **1**, 27-31. <http://dx.doi.org/10.4236/ait.2011.12004>
- [15] (2005) ITU Internet Reports, International Telecommunication Union. The Internet of Things: 7th Edition. [www.itu.int/internetofthings/on](http://www.itu.int/internetofthings/on)
- [16] Want, R. (2006) An Introduction to RFID Technology. *IEEE Pervasive Computing*, **5**, 25-33.
- [17] Li, B.A. and Yu, J.J. (2011) Research and Application on the Smart Home Based on Component Technologies and Internet of Things. *Procedia Engineering*, **15**, 2087-2092. <http://dx.doi.org/10.1016/j.proeng.2011.08.390>
- [18] Razzak, F. (2012) Spamming the Internet of Things: A Possibility and its probable Solution. *Procedia Computer Science*, **10**, 658-665. <http://dx.doi.org/10.1016/j.procs.2012.06.084>
- [19] Shao, W. and Li, L. (2009) Analysis of the Development Route of IoT in China. *Perking: China Science and Technology Information*, **24**, 330-331.
- [20] Sun, C. (2012) Application of RFID Technology for Logistics on Internet of Things.
- [21] Moeinfar, D., Shamsi, H. and Nafar, F. (2012) Design and Implementation of a Low-Power Active RFID for Container Tracking @ 2.4 GHz Frequency: Scientific Research.

- 
- [22] Bicknell, IPv6 Internet Broken, Verizon Route Prefix Length Policy, 2009.
  - [23] Grieco A., Occhipinti, E. and Colombini, D. (1989) Work Postures and Musculo-Skeletal Disorder in VDT Operators. *Bollettino de Oculistica*, Suppl. 7, 99-111.
  - [24] Pahlavan, K., Krishnamurthy, P., Hatami, A., Ylianttila, M., Makela, J.P., Pichna, R. and Vallstron, J. (2007) Handoff in Hybrid Mobile Data Networks. *Mobile and Wireless Communication Summit*, 7, 43-47.
  - [25] Chen, X.-Y. and Jin, Z.-G. (2012) Research on Key Technology and Applications for the Internet of Things. *Physics Procedia*, 33,561-566. <http://dx.doi.org/10.1016/j.phpro.2012.05.104>
  - [26] Arampatzis, T., *et al.* (2005) A Survey of Security Issues in Wireless Sensors Networks, in Intelligent Control. *Proceeding of the IEEE International Symposium on, Mediterrean Conference on Control and Automation*, 719-724.
  - [27] Chorost, M. (2008) The Networked Pill, MIT Technology Review, March.