

Internet of Things (IoT): A Review of the Literature

Dr. Ranjan Kumar Mondal

Assistant Professor, Department of CSE, Swami
Vivekananda University, Kolkata, WB
ranjankm@svu.ac.in

Synopsis

The Internet of Things (IoT) is one of the hottest terms in information technology. The Internet of Things (IoT) will convert physical things into intelligent virtual ones in the future. The Internet of Things (IoT) seeks to bring everything in our world together under a single infrastructure, providing us with both control over the objects in our environment and real-time information on their condition. The current study systematically evaluates academic research publications, business white papers, expert interviews, and internet databases to address IoT principles. Additionally, the main topics of this study paper are the definitions, genotypes, prerequisites, traits, and aliases of the Internet of Things. This paper's primary goal is to provide an overview of the Internet of Things, key technologies, and their applications in day-to-day living. Nonetheless, this work will aid in efficiently acquiring information and provide new researchers with a solid understanding of their study in the Internet of Things (Technological GOD).

Keywords

Wi-Fi, Bluetooth, NFC, ZigBee, RFID, IPv6, EPC, barcode, sensors, actuators, and the Internet of Things

1. Overview

"The technologies that vanish are the most significant. The main thesis of Mark Weiser's landmark 1991 study [Weis 91] in Scientific American was, "They weave themselves into the fabric of everyday life until they are indistinguishable

from it.” With the introduction of IT and IT technologies, human existence and working circumstances in enterprises have undergone a radical transformation. Due to its many applications, this idea is becoming increasingly well-known in both horizontal and vertical markets and the daily lives of the average person in society. Large organizations have been the main force behind the development of the Internet of Things (IoT) since they stand to gain a great deal from the predictability and foresight of tracking every item through the commodity chains in which they are enmeshed [1]. Through IoT, businesses have been able to integrate sophisticated and adaptable organizational systems, expedite procedures, lower mistake rates, prevent theft, and become more efficient thanks to the capacity to code and monitor items [2]. The Internet of Things (IoT) is a technological revolution that will shape computers and communications in the future. Its growth relies on rapid technological advancement in several key areas, including nanotechnology and wireless sensors. They will tag each item for

It is recognizing, automating, keeping an eye on, and managing.

2.The Internet of Things

Within the IT industry, the Internet of Things represents a new paradigm. The two terms “Internet” and “things,” which come from the first and second words, respectively, are combined to form the phrase “Internet of Things,” or IoT. The Internet is a global network of linked computer networks that provide services to billions of users worldwide using the standard Internet protocol suite (TCP/IP). It comprises millions of local to international private, public, academic, corporate, and government networks connected by a wide range of electrical, wireless, and optical networking technologies [3]. These days, the Internet connects more than 100 nations to facilitate sharing information, news, and viewpoints. An estimated 2 267 233 742 people were using the Internet globally as of December 31, 2011, according to Internet World Statistics (statistics accessed on June 6, 2013, from the Universal Resource Location <http://www.webopedia.com/TERM/I/Internet.html>). This indicates that

32.7% of people on the planet use the Internet. In the next four years, even the Internet will go into space thanks to Cisco's Internet Routing in Space (IRIS) initiative (Accessed on October 5, 2012: <http://www.cisco.com/web/strategy/government/space-routing.html>). When it comes to the Things, they may be any person or thing that the actual world can tell apart. In addition to the electronic devices we use daily and the technologically advanced products like gadgets and equipment, everyday objects also include "things" that we would not typically consider to be electronic, like food, clothing, and furniture; materials, parts, and equipment; merchandise; specialized items; landmarks; monuments; and works of art, as well as all the various aspects of commerce, culture, and sophistication [4]. This indicates that objects may be non-living items like chairs, refrigerators, tube lights, curtains, plates, and other household equipment, as well as live objects like people, animals (cows, calves, dogs, pigeons, rabbits, etc.), and plants (mango trees, jasmine, banyan, etc.). Things are now considered objects in this material or physical universe.

2.1. Definitions

The global user community does not yet have a single, widely accepted meaning for the term "Internet of Things." Although the term's first usage was credited to digital innovation specialist Kevin Ashton, many distinct organizations have defined it, including academics, researchers, practitioners, innovators, developers, and business individuals. The premise that data generated by humans was the focus of the first iteration of the Internet and data created by objects was the common denominator throughout all the definitions. The following is the best definition of the Internet of Things:

"An extensive and open network of intelligent objects with the ability to self-organize, exchange data and resources, and respond and act in response to external events and changes."

The Internet of Things is still the newest and most talked-about idea in the IT industry, but it is starting to mature. The phrase "Internet of Things" (IoT) gained popularity over the last ten years because it presents the idea of a global infrastructure

made up of physically connected things that can be connected at any time and from any location to anything [4]. The Internet of objects may also be considered a worldwide network that gives every item a unique identity, enabling communication between humans, objects, and anything else in the world [5]. The Internet of Things (IoT) envisions a society in which almost everything is linked and capable of intelligent communication. Most associate “being connected” with modern gadgets like computers, tablets, phones, servers, and smartphones. “Internet of Things” refers to wired and wireless networks that link sensors and actuators built into physical things, such as pacemakers and roads, often utilizing the same Internet Protocol (IP) that links the Internet. These networks produce Massive amounts of data and send it to computers for processing. When an item can perceive its surroundings and communicate, it may be used to quickly and efficiently comprehend complexity. The revolutionary aspect is that these physical information systems are already being implemented; some even function primarily without human interaction. The coding and networking of commonplace items to make each one uniquely machine-readable and traceable online is referred to as the “Internet of Things” [6]–[11]. Coded RFID tags and IP addresses connected to an EPC (Electronic Product Code) network are the primary means of creating most of the material now available on the Internet of Things [12].

2.2.Genesis

The Internet of Things represents the future of computing and communications, a technological revolution whose growth depends on rapid technological advancement in several critical areas, including nanotechnology and wireless sensors (Accessed dated on 20/04/2013 from URL: <http://www.ieccr.net/comsoc/ijcis/>). Early in the 1980s, a Coke machine at Carnegie Mellon University served as the first Internet appliance. A server application that tracked the time since a storage column in the vending machine had been empty was created by programmers working several stories above the machine. Should they want to trek down to the machine, the programmers could use the Internet to connect to it, check its condition, and find out whether a cool drink

would be waiting for them. Although “Internet of Things” first appeared about coffee vending machines in the 1980s, Kevin Ashton, the Executive Director of Auto-ID Labs at MIT, is credited with coining the original term in 1999. The Auto-ID Center in 2003 and writings by associated market analysts helped popularize the idea of the Internet of Things for the first time. From the outset of the development of the Internet of Things, a wide range of items and objects were linked to the network for various purposes using various technologies, depending on the kind of object and how comfortable humans might be with it.

3.Sequence of Time

obtained from <http://postscapes.com/internet-of-things-history>, which was last accessed on March 24, 2013.

1999: Kevin Ashton, Executive Director of the Auto-ID Center at Massachusetts Institute of Technology (MIT), created the phrase “Internet of Things.”

1999: Kevin Ashton, David Brock, and Sanjay Sarma founded the MIT Auto-ID Lab this year. Neil Gershenfeld initially discussed IoT ideas in his book *When Things Start to Think* in 1999.

They contributed to the development of the Electronic Product Code.

2000 saw LG unveil its first Internet of Refrigerator initiatives.

2002 saw the public debut of the Ambient Orb, a spin-off from the MIT Media Lab developed by David Rose and colleagues. NY Times Magazine named it one of the Ideas of the Year.

(2003–2004): The US Department of Defense, via the Savi program, and Wal-Mart, in the private sector, heavily use RFID.

The UN released the International Telecommunication Union’s (ITU) first report on the Internet of Things in 2005.

2008: The first European IoT conference is conducted, and the EU recognizes

In 2008, several businesses founded the IPSO Alliance to advance IP usage in “smart object” networks and facilitate the Internet of Things.

2008: Cisco’s Business Solutions Group claims that the Internet of Things was created when the FCC voted 5-0 to allow opening the use of the “white space” spectrum (2008–2009).

The Internet of Things (IoT) was named one of the six “Disruptive Civil Technologies” by the US National Intelligence Council in 2008. It may affect US interests until 2025.

2010: Chinese Premier Wen Jiabao aims to make significant investments in the Internet of Things and describes it as a crucial business for China.

Public introduction of IPv6 in 2011: The new protocol permits 340, 282, 366, 920, 938, 463, 463, 374, 607, 431,768,

Addresses 211, 456 (2128)

2.4.Aliens

Although the term “Internet of Things” is used differently by various individuals, the general goal of the concept remains the same. Web of Things, Internet of Objects, Embedded Intelligence, Connected Devices, and Technology Omnipotent, Omniscient, and Omnipresent are other names for the Internet of Things. Along with these, it has also been referred to as (1) Cyber-Physical Systems, or “Integrations of computation and physical processes,” which merge the virtual and physical worlds; (2) Pervasive Computing, or a computer environment where virtually everything has processing power with wired or wireless connections to a global network; (3) Ubiquitous Computing, also known as “Calm technology,” which refers to the state in which technology is practically invisible in our daily lives; (4) Machine-to-Machine Interaction, or minimal human intervention while devices are communicating end-to-end; (5) Human-Computer Interaction, or the study, planning, and design of human-computer interaction.

A new technology called ambient intelligence will make our daily environment more responsive and sensitive.

2.5.Conditions

Achieving a successful Internet of Things (IoT) implementation requires several prerequisites, including (a) dynamic resource demand, (b) real-time needs, (c) exponential growth in demand, (d) application availability, (e) data protection and user privacy; (f) efficient power consumption of applications; (g) application execution close to end users; and (h) access to an open and interoperable cloud system.

Three elements are necessary for seamless Internet of Things (IoT) computing, according to another author: (a) Hardware, which consists of sensors, actuators, IP cameras, CCTV, and embedded communication hardware; (b) Middleware, which includes on-demand storage and computing tools for data analytics with cloud and Big Data Analytics; and (c) Presentation, which consists of simple visualization and interpretation tools that can be tailored for various applications.

2.6.The hype cycle of Gartner

Gartner's Information Technology Hype Cycle [13] visualizes the emergence, adoption, maturity, and impact on applications of particular technologies. (2) In the following graph, the X-axis represents expectations, and the Y-axis represents time factors. (3) According to Gartner's IT Hype Cycle, the Internet of Things has been identified as one of the emerging technologies. (4) As of 2012, it has been predicted that IoT will take approximately 5 to 10 years to become widely adopted. For information, see the image.

3.Structures

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

The lack of a standardized architecture for the Internet of Things is one of its primary issues since it is such a big and abstract idea. For the Internet of Things to function, various sensors, networks, communications, and computer technologies are required [14]. Multiple writers, researchers, and practitioners provide several IoT models or architectures.

3.1.European Research Project (FP7)

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

3.2.ITU Architecture

The International Telecommunication Union (ITU) has recommended that the Internet of Things network architecture contains :

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

Regarding networks and data transfer, they are comparable to the Open Systems Interconnection (OSI) reference model.

3.3.IoT Forum Structure

According to the IoT Forum, applications, Processors, and Transpiration are the three core categories into which the Internet of Things Architecture is divided.

3.4.Architecture by Zhang Jidong and Qian Xiaocong

Qian Xiaocong and Zhang Jidong (2012) state that three levels comprise the conventional Internet of Things. At the bottom, the perception layer is responsible for object cognition and information gathering. Each carrier's OFC, mobile phone networks, fixed phone networks, broadcasting networks, and closed IP data networks comprise the intermediate transportation layer. Lastly, the application layer sits on top, where many applications operate. Smart traffic, precise agriculture, intelligent logistics, smart industrial, environment protection, mining monitoring, remote nursing, safety defense, competent government, etc., are examples of typical applications included in this layer.

3.5.The Architecture of Kun Han, Shurong Liu, Dacheng Zhang, and Ying Han (2012)

The model used in “First Studies for the Development of SSME under the Background of IoT” is

4.Technology

Members of the RFID community first mentioned the possibility of finding out information about a tagged object by looking up an internet address or database entry that matched a specific RFID or Near Field Communication [16] technology. This idea served as the inspiration for the Internet of Things [15]. Key IoT technologies included in the study paper “Research and application on the smart home based on component technologies and Internet of Things” include RFID, sensor technology, nanotechnology, and intelligence embedded technology. RFID is the cornerstone and networking hub of the Internet of Things, among other things [17]. Users can now integrate actual devices into the virtual world thanks to the Internet of Things (IoT). Various tagging technologies, such as NFC, RFID, and 2D barcode, enabled the identification and referral of physical things over the internet, making this practical [18]. The Internet of Things (IoT) is the collective name for the ubiquitous network built on the ever-present hardware resources of the Internet, which is merged with radio frequency and sensor technology. Additionally, using computing fields, communication networks, and global roaming technology has created a new wave in the IT business. It involves many new Internet of Things supporting technologies, such as collecting information technology, remote communication technology, remote information transmission technology, sea measures information intelligence analysis, controlling technology, and sophisticated computer and communication network outside technologies [19].

4.1.Identification of Radio Frequencies (RFID)

Radio Frequency Identification (RFID) uses radio waves to wirelessly broadcast an item or person’s identity as a serial number [20]. In 1948, the first RFID gadget was deployed in Britain during World War II to identify friends and foes.

Subsequently, in 1999, the Auto-ID Center at MIT established RFID technology. In the Internet of Things, RFID technology is crucial for resolving identifying problems.

Of the things in our environment in an economical way [5]. RFID technology can be divided into three categories: Active, passive, and semi-passive. The tag, reader, antenna, access controller, software, and server are the significant components of RFID. It is more accurate, cost-effective, safe, and dependable. RFID has a wide variety of wireless applications, including uses for the military, tracing, distribution, and medical monitoring [21].

4.2. Protocol for the Internet (IP)

The primary network protocol used on the Internet is called Internet Protocol (IP), and it was created in the 1970s. The Internet protocol suite's primary communications protocol, or IP, transmits datagrams across network borders. IPv4 and IPv6 are the two versions of Internet Protocol (IP) currently in use. An IP address is defined differently in each version. The addresses specified by IPv4 are nevertheless often referred to by the general name IP address due to their widespread use. While only classes A, B, and C are frequently utilized, there are five classes of possible IP ranges in IPv4: classes A, B, C, D, and E. While IPv6 would significantly increase the availability to 85,000 trillion addresses, the current protocol only allows for 4.3 billion IPv4 addresses [22]. The 21st-century Internet Protocol is called IPv6. This is compatible with around 2¹²⁸ addresses.

4.3. Code for Electronic Products (EPC)

The Electronic Product Code (EPC) aims to designate an enhancement in the EPC barcode system. It is a 64- or 98-bit code electronically encoded on an RFID tag. Information regarding the kind of EPC, the product's unique serial number, its specs, the manufacturer, and other details may all be included in the EPC code. The Auto-ID Center at MIT created EPC in 1999. The Electronic Product Code (EPC) technology standards body, EPCglobal Organisation [Wikipedia, "EPCglobal," 2010], established the EPCglobal Network [Wikipedia, "EPCglobal Network," 2010] to

facilitate the exchange of RFID data. Object Naming Service (ONS), EPC Discovery Service (EPCDS), EPC Information Services (EPCIS), and EPC Security Services (EPCSS) are its four constituent parts.

4.4.Barcode

A barcode is an alternative method of encoding characters and numbers consisting of bars and gaps with varying widths. Although not essential, Behind Bars [23] fulfills its initial purpose of being descriptive. Palmer (1995) recognizes the existence of alternate data input strategies in The Bar Code Book. The trademark for a particular kind of matrix barcode that was first created for the Japanese car sector is the Quick Response (QR) Code. Bar codes are optical, machine-readable labels affixed to objects and contain information about them. Because of the QR Code system's quicker reading and larger storage capacity than traditional codes, it has gained popularity outside the automobile sector. Barcodes come in three varieties: two-dimensional, numeric, and alphanumeric. Barcodes are intended to be readable by machines. Although cameras may also scan them, laser scanners are often used to read them.

4.5.Wireless Communication (Wi-Fi)

Using a wireless signal, computers, and other devices may interact thanks to a networking technology called wireless fidelity, or WiFi. The man credited with inventing wireless fidelity is Vic Hayes. NCR Corporation introduced the Wi-Fi forerunner in 1991 in Nieuwege, the Netherlands. With speeds ranging from 1 Mbps to 2 Mbps, the first wireless solutions were released into the market under WaveLAN. These days, Wi-Fi is almost universal, providing high-speed Wireless Local Area Network (WLAN) connection to millions of homes, workplaces, and public spaces like cafés, hotels, and airports. The popularity of Wi-Fi has increased to the point that it is almost standard in laptops, handheld devices, and Consumer Electronics (CE) products [24]. Technology includes all WLAN equipment types that support IEEE.

In addition to dual-band 802.11, there are also 802.11a, 802.11b, 802.11g, and 802.11n. These days, wireless APs are turning whole cities into Wi-Fi corridors.

4.6. Bluetooth

The low-cost, short-range radio technology known as Bluetooth wireless technology eliminates the need for professionals.

Primary cabling with an effective range of 10 to 100 meters connecting gadgets such as laptop PCs, portable PCs, PDAs, cameras, and printers. Bluetooth employs the IEEE 802.15.1 standard specification; most communication occurs at less than 1 Mbps. The Ericson Mobile Communication Company launched the “Bluetooth” idea in 1994. Network construction using it is done for Personal Area Networks (PAN). A Piconet is a group of Bluetooth devices communicating over a single channel. This Piconet can share data with two to eight devices simultaneously. Text, images, videos, and sounds may all be included in the data. More than a thousand businesses, including Ericson, IBM, Motorola, Toshiba, Cisco, HP, Aruba, and Intel, are Bluetooth Special Interest Group members.

4.7. ZigBee

One of the technologies created to improve wireless sensor network functionality is called ZigBee. The ZigBee Alliance was established in 2001 and is responsible for creating ZigBee technology. Low cost, low data rate, short transmission range, scalability, dependability, and adaptable protocol architecture are some of ZigBee’s features. Based on IEEE 802.15.4, it is a low-power wireless network protocol [25]. ZigBee operates in star, cluster tree, and mesh topologies and has a range of around 100 meters and a bandwidth of 250 kbps. It is extensively used in power systems, digital agriculture, industrial controls, home automation, and medical monitoring.

4.8. Close Filed Exchange (NFC)

A typical distance of 4 cm is needed for Near Field Communication (NFC), a collection of short-range wireless technologies operating at 13.56 MHz. With NFC technology, people all over the globe may link electronic devices with a touch, exchange digital content, and complete transactions more easily and conveniently. It enables simple wireless network setup, and NFC’s long-range capabilities at up

to 10 cm make it an excellent supplement to Bluetooth and 802.11. It also has a quick and straightforward connecting mechanism, doesn't need a line of sight, and operates in unclean environments. The firms Philips and Sony developed it first. The current Data exchange rate is around 424 kbps. In NFC, power consumption is less than 15ma for reading data.

4.9.Activators

Actuators drive movements into mechanical systems by converting energy into motion. It requires power from an electric current, hydraulic fluid, or another source. Actuators can produce oscillatory, rotational, or linear motion. Typically, they travel up to 30 feet over short distances and communicate at a speed of less than 1 Mbps. Actuators are often used in industrial or manufacturing settings. Three different kinds of actuators exist: (1) Electrical, which includes stepper motors, AC and DC motors, and solenoids; (2) Hydraulic, which uses hydraulic fluid to actuate motion; and (3) Pneumatic, which uses compressed air. These three categories of actuators are still widely used in modern times. Electric actuators are the most often utilized kind among them. Pneumatic and hydraulic systems enable smaller motors to provide more force and torque.

4.10.Networks of Wireless Sensors (WSN)

According to Wikipedia, a wireless sensor network (WSN) is a network of geographically dispersed autonomous devices that work together to cooperatively monitor various physical and environmental factors, including motion, temperature, sound, vibration, pressure, and pollution—composed of thousands or even hundreds of motes that exchange information and converse with one another. A wireless sensor network is vital to the concept of the Internet of Things. Due to the high overhead and volume of sensors, sensor nodes could not have global ID. The military, homeland security, healthcare, manufacturing, habitat monitoring, precision agricultural monitoring, forest fire, flood detection, and many other fields have shown great interest in WSN based on IoT [26]. Doctors may quantify the impact of medications by monitoring the reactions to such medications with sensors attached to the patient's body [27].

4.11.Human-machine intelligence (AI)

Electronic environments that are aware of and react to human presence are called artificial intelligence. In a world with ambient intelligence, gadgets cooperate to help people go about their daily lives.

Day-to-day tasks are simple and organic, using intelligence and information concealed in network-connected gadgets. Embedded: A lot of networked devices are integrated into the environment; (2) Context-Aware: These devices can identify you and your situational context; (3) Personalized: They can be customized to meet your needs; (4) Adaptive: They can adjust to your needs; and (5) Anticipatory: They can predict your desires without conscious mediation.

Conclusion

Through various technologies and applications, the Internet of Things has progressively brought about a sea of technical changes in our everyday lives, making our lives easier and more pleasant. The Internet of Things has many applications in every field, including government, education, healthcare, manufacturing, mining, and housing. Despite all of the advantages of IoT, there are several shortcomings in implementation and control. The literature's main findings are as follows: (1) There is no universal definition; (2) Universal standardizations are needed at the architectural level; (3) Technologies vary from vendor to vendor; and (4) Standard protocols must be developed to improve global governance. Let's hope for better IoT in the future.

References

- 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>
- 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.

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>

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.

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*.

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>

Lombreglia, R. (2010) The Internet of Things, Boston Globe. Retrieved October. [11] Reinhardt, A. (2004) A Machine-to-Machine Internet of Things.

Graham, M. and Haarstad, H. (2011) Transparency and Development: Ethical Consumption through Web 2.0 and the Internet of Things. *Research Article*, **7**.

Jayavardhana, G., Rajkumar, B., Marusic, S. and Palaniswami, M. (2013) Internet of Things: A Vision, Architectural Elements, and Future Directions. Future Generation.

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>

(2005) ITU Internet Reports, International Telecommunication Union. The Internet of Things: 7th Edition. www.itu.int/internetofthings/on

Want, R. (2006) An Introduction to RFID Technology. *IEEE Pervasive Computing*, **5**, 25-33.

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>

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>

Shao, W. and Li, L. (2009) Analysis of the Development Route of IoT in China. *Parking: China Science and Technology Information*, **24**, 330-331.

Sun, C. (2012) Application of RFID Technology for Logistics on Internet of Things.

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.

Bicknell, IPv6 Internet Broken, Verizon Route Prefix Length Policy, 2009.

Grieco A., Occhipinti E. and Colombini, D. (1989) Work Postures and Musculo-Skeletal Disorder in VDT Operators. *Bollettino de Oculistica*, Suppl. 7, 99-111.

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.

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>

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.