

A Review on Internet of Things (IoT)

M.U. Farooq

Electronic Engineering Department
PAF-Karachi Institute of
Economics & Technology,
Pakistan

Muhammad Waseem

Telecomm. Engineering Department
Sir Syed University of
Engineering & Technology,
Pakistan

Sadia Mazhar

Electrical Engineering Department
Sir Syed University of
Engineering & Technology,
Pakistan

Anjum Khairi

Electronic Engineering Department
Sir Syed University of
Engineering & Technology,
Pakistan

Talha Kamal

Bio Medical Engineering Department
Sir Syed University of
Engineering & Technology,
Pakistan

ABSTRACT

Internet, a revolutionary invention, is always transforming into some new kind of hardware and software making it unavoidable for anyone. The form of communication that we see now is either human-human or human-device, but the Internet of Things (IoT) promises a great future for the internet where the type of communication is machine-machine (M2M). This paper aims to provide a comprehensive overview of the IoT scenario and reviews its enabling technologies and the sensor networks. Also, it describes a six-layered architecture of IoT and points out the related key challenges.

Keywords:

Internet of Things, RFID, WSN, IOT architecture, IoT Vision, IoT applications, IoT security.

1. INTRODUCTION

With the continuous advancements in technology a potential innovation, IoT is coming down the road which is burgeoning as an ubiquitous global computing network where everyone and everything will be connected to the Internet [1]. IoT is continually evolving and is a hot research topic where opportunities are infinite. Imaginations are boundless which have put it on the verge of reshaping the current form of internet into a modified and integrated version. The number of devices availing internet services is increasing every day and having all of them connected by wire or wireless will put a powerful source of information at our finger tips. The concept of enabling interaction between intelligent machines is a cutting-edge technology but the technologies composing the IoT are not something new for us [2]. IoT, as you can guess by its name, is the approach of converging data obtained from different kinds of things to any virtual platform on existing Internet infrastructure [3].

The concept of IoT dates back to 1982 when a modified coke machine was connected to the Internet which was able to report the drinks contained and that whether the drinks were cold [4]. Later, in 1991, a contemporary vision of IoT in the form of ubiquitous

computing was first given by Mark Weiser [5]. However in 1999, Bill Joy gave a clue about Device to Device communication in his taxonomy of internet [6]. In the very same year, Kevin Ashton proposed the term "Internet of Things" to describe a system of interconnected devices [7].

The basic idea of IoT is to allow autonomous exchange of useful information between invisibly embedded different uniquely identifiable real world devices around us, fueled by the leading technologies like Radio-Frequency IDentification (RFID) and Wireless Sensor Networks (WSNs) [2] which are sensed by the sensor devices and further processed for decision making, on the basis of which an automated action is performed [1].

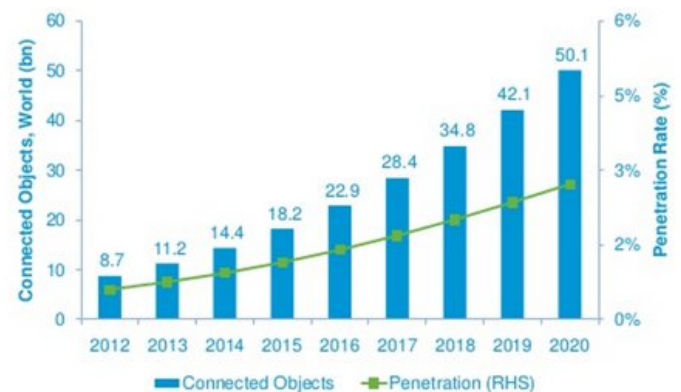


Fig. 1. Expected penetration of connected objects by the year 2020, according to Cisco

The paper is organized as follows. Section 2 analyzes the vision of the IoT. Section 3 describes the generic architecture of the IoT. Section 4 discusses the technologies that IoT is composed of. Section 5 forecasts the future applications. Section 6 discusses the privacy

and security challenges posed by IoT and finally Section 7 concludes the paper.

2. VISION

In 2005, ITU reported about a ubiquitous networking era in which all the networks are interconnected and everything from tires to attires will be a part of this huge network [8]. Imagine yourself doing an internet search for your watch you lost somewhere in your house. So this is the main vision of IoT, an environment where things are able to talk and their data can be processed to perform desired tasks through machine learning [9]. A practical implementation of IoT is demonstrated by a soon-to-be released Twine, a compact and low-power hardware working together with real-time web software to make this vision a reality [10]. However different people and organizations have their own different visions for the IoT [11].

An article published in Network World revealed IoT strategies of top IT vendors, they carried out some interviews from the key IT vendors. As of HP's vision, they see a world where people are always connected to their content. Cisco believes in the industrial automation and convergence of operational technology. Intel is focused on empowering billions of existing devices with intelligence. Microsoft does not consider IoT as any futuristic technology; they believe that it already exists in today's powerful devices and that the devices just need to be connected for a large amount of information which could be helpful. While, IBM has a vision of a Smarter Planet by remotely controlling the devices via secured servers [12].

Despite of having different visions, they all agree about a network of interconnected devices therefore more developments within the coming decades are expected to be seen including that of a new converged information society [13].

3. ARCHITECTURE

More than 25 Billion things are expected to be connected by 2020 [14] which is a huge number so the existing architecture of Internet with TCP/IP protocols, adopted in 1980 [15], cannot handle a network as big as IoT which caused a need for a new open architecture that could address various security and Quality of Service (QoS) issues as well as it could support the existing network applications using open protocols [16]. Without a proper privacy assurance, IoT is not likely to be adopted by many [17]. Therefore protection of data and privacy of users are key challenges for IoT [18].

For further development of IoT, a number of multi-layered security architectures are proposed. [19] described a three key level architecture of IoT while [20] described a four key level architecture. [21] proposed a five layered architecture using the best features of the architectures of Internet and Telecommunication management networks based on TCP/IP and TMN models respectively. Similarly a six-layered architecture was also proposed based on the network hierarchical structure [22]. So generally it's divided into six layers as shown in the Fig. 2.

The six layers of IoT are described below:

3.1 Coding Layer

Coding layer is the foundation of IoT which provides identification to the objects of interest. In this layer, each object is assigned a unique ID which makes it easy to discern the objects [22].

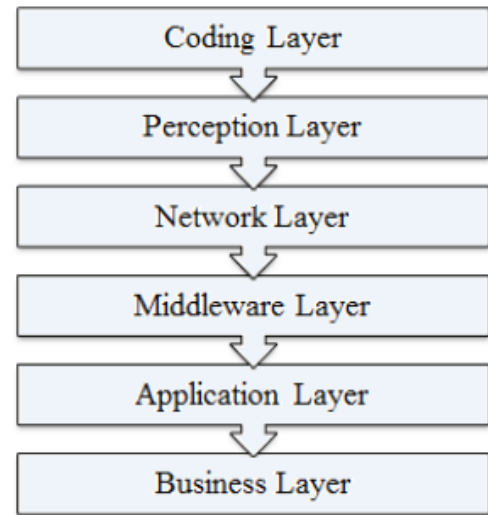


Fig. 2. Six-Layered Architecture of IoT

3.2 Perception Layer

This is the device layer of IoT which gives a physical meaning to each object. It consists of data sensors in different forms like RFID tags, IR sensors or other sensor networks [23] which could sense the temperature, humidity, speed and location etc of the objects. This layer gathers the useful information of the objects from the sensor devices linked with them and converts the information into digital signals which is then passed onto the Network Layer for further action.

3.3 Network Layer

The purpose of this layer is receive the useful information in the form of digital signals from the Perception Layer and transmit it to the processing systems in the Middleware Layer through the transmission mediums like WiFi, Bluetooth, WiMaX, Zigbee, GSM, 3G etc with protocols like IPv4, IPv6, MQTT, DDS etc [24].

3.4 Middleware Layer

This layer processes the information received from the sensor devices [2]. It includes the technologies like Cloud computing, Ubiquitous computing which ensures a direct access to the database to store all the necessary information in it. Using some Intelligent Processing Equipment, the information is processed and a fully automated action is taken based on the processed results of the information.

3.5 Application Layer

This layer realizes the applications of IoT for all kinds of industry, based on the processed data. Because applications promote the development of IoT so this layer is very helpful in the large scale development of IoT network [21]. The IoT related applications could be smart homes, smart transportation, smart planet etc.

3.6 Business Layer

This layer manages the applications and services of IoT and is responsible for all the research related to IoT. It generates different business models for effective business strategies [1].

4. TECHNOLOGIES

The development of a ubiquitous computing system where digital objects can be uniquely identified and can be able to think and interact with other objects to collect data on the basis of which automated actions are taken, requires the need for a combination of new and effective technologies which is only possible through an integration of different technologies which can make the objects to be identified and communicate with each other [25]. In this section we discuss the relevant technologies that can help in the large-scale development of IoT.

4.1 Radio Frequency Identification (RFID)

RFID is the key technology for making the objects uniquely identifiable. Its reduced size and cost makes it integrable into any object [19]. It is a transceiver microchip similar to an adhesive sticker which could be both active and passive, depending on the type of application [26]. Active tags have a battery attached to them due to which they are always active and therefore continuously emit the data signals while Passive tags just get activated when they are triggered. Active tags are more costly than the Passive tags however they have a wide range of useful applications [2]. RFID system is composed of readers and associated RFID tags which emit the identification, location or any other specifics about the object, on getting triggered by the generation of any appropriate signal [27]. The emitted object related data signals are transmitted to the Readers using radio frequencies which are then passed onto the processors to analyze the data.

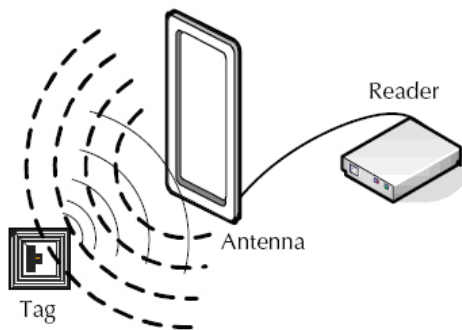


Fig. 3. RFID Scenario

Depending on the type of application, RFID frequencies are divided into four different frequencies ranges [28], which are given below:

- (1) Low frequency (135 KHz or less)
- (2) High Frequency (13.56MHz)
- (3) Ultra-High Frequency (862MHz - 928MHz)
- (4) Microwave Frequency (2.4G , 5.80)

Bar Code is also an identification technology which has almost the same function as an RFID but RFID is more effective than a Bar Code due to a number of its benefits. RFID being a radio technology doesn't require the reader to be physically in its vision while Bar Code is an optical technology which cannot work unless its reader is placed in front of it. Moreover, an RFID can work as an actuator to trigger different events and it has even modification abilities which Bar codes clearly don't have.

4.2 Wireless Sensor Network (WSN)

WSN is a bi-directional wirelessly connected network of sensors in a multi-hop fashion, built from several nodes scattered in a sensor field each connected to one or several sensors which can collect the object specific data such as temperature, humidity, speed etc and then pass on to the processing equipment [26]. The sensing nodes communicate in multi-hop. Each sensor is a transceiver having an antenna, a micro-controller and an interfacing circuit for the sensors as a communication, actuation and sensing unit respectively along with a source of power which could be both battery or any energy harvesting technology [29]. However [2] has proposed an additional unit for saving the data, named as Memory Unit which could also be a part of the sensing node. A typical sensing node is shown in the figure below:

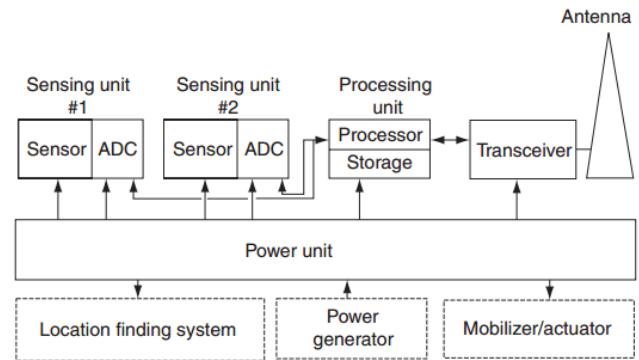


Fig. 4. A typical sensing node

Wireless Sensors Network technology and RFID technology when combined together opens up possibilities for even more smart devices, for which a number of solutions have been proposed [26]. An example solution is provided by the Intel Research Labs in the form of Wireless Identification Sensing Platform (WISP) [30]. WISP is a passive wireless sensor network with built-in light, temperature and many other sensors [31]. Both WSN and RFID Sensor Networks have their own advantages but RFID Sensor Networks have a low range and their communication is Asymmetric while WSNs have a comparatively longer range and their communication is Peer-to-Peer. Moreover most of the WSNs are based on the IEEE 802.15.4 standard [26], which specifies the Physical and MAC layer of Low-Rate Wireless Personal Area Networks (LR-WPANs) [32].

The technologies that enables the integration of WSN with the IOT are a hot research topic, many solutions have been proposed for that including that of a 6LOWPAN standard [33], that allows IPv6 packets to be transmitted through the networks that are computationally restricted. Also there's ROLL routing standard for end-to-end routing solutions [34].

4.3 Cloud Computing

With millions of devices expected to come by 2020 [14], the cloud seems to be the only technology that can analyze and store all the data effectively. It is an intelligent computing technology in which number of servers are converged on one cloud platform to allow sharing of resources between each other which can be accessed at

any time and any place [35]. Cloud computing is the most important part of IoT, which not only converges the servers but also processes on an increased processing power and analyzes the useful information obtained from the sensors and even provide good storage capacity [36]. But this is just a beginning of unleashing the true potential of this technology. Cloud computing interfaced with smart objects using potentially millions of sensors can be of enormous benefits and can help IoT for a very large scale development so researches are being carried out since IoT will be totally dependent on the Cloud Computing.

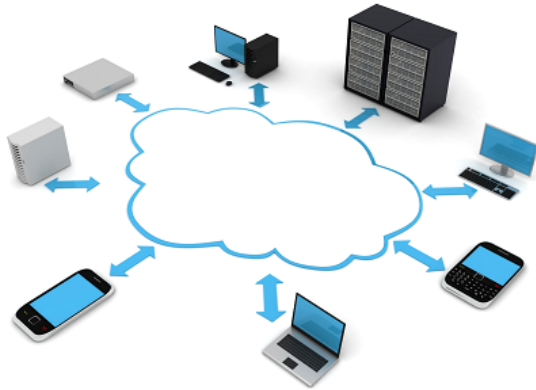


Fig. 5. A typical Cloud Computing Scenario

4.4 Networking Technologies

These technologies have an important role in the success of IoT since they are responsible for the connection between the objects, so we need a fast and an effective network to handle a large number of potential devices. For wide-range transmission network we commonly use 3G, 4G etc. but As we know, mobile traffic is so much predictable since it only has to perform the usual tasks like making a call, sending a text message etc. so as we step into this modern era of ubiquitous computing, it will not be predictable anymore which calls for a need of a super-fast, super-efficient fifth generation wireless system which could offer a lot more bandwidth [37]. Similarly for a short-range communication network we use technologies like Bluetooth, WiFi etc.

4.5 Nano Technologies

This technology realizes smaller and improved version of the things that are interconnected. It can decrease the consumption of a system by enabling the development of devices in nano meters scale which can be used as a sensor and an actuator just like a normal device. Such a nano device is made from nano components and the resulting network defines a new networking paradigm which is Internet of Nano-Things [38].

4.6 Micro-Electro-Mechanical Systems (MEMS) Technologies

MEMS are a combination of electric and mechanical components working together to provide several applications including sensing and actuating which are already being commercially used in many field in the form of transducers and accelerometers etc. MEMS

combined with Nano technologies are a cost-effective solution for improvising the communication system of IoT and other advantages like size reduction of sensors and actuators, integrated ubiquitous computing devices and higher range of frequencies etc [39].

4.7 Optical Technologies

Rapid developments in the field of Optical technologies in the form of technologies like Li-Fi and Cisco's BiDi optical technology could be a major breakthrough in the development of IoT. Li-Fi, an epoch-making Visible Light Communication (VLC) technology, will provide a great connectivity on a higher bandwidth for the objects interconnected on the concept of IoT. Similarly Bi-Directional (BiDi) technology gives a 40G ethernet for a big data from multifarious devices of IoT [40].

5. APPLICATIONS

Most of the daily life applications that we normally see are already smart but they are unable to communicate with each other and enabling them to communicate with each other and share useful information with each other will create a wide range of innovative applications [41]. These emerging applications with some autonomous capabilities would certainly improve the quality of our lives. A few of such applications are already in the market [26], let's take the example of the Google Car which is an initiative to provide a self-driving car experience with real-time traffic, road conditions, weather and other information exchanges [42], all due to the concept of IoT. There are a number of possible future applications that can be of great advantage. In this section, we present few of these applications.

5.0.1 Smart Traffic System. Traffic is an important part of a society therefore all the related problems must be properly addressed. There is a need for a system that can improve the traffic situation based on the traffic information obtained from objects using IoT technologies [43]. For such an intelligent traffic monitoring system, realization of a proper system for automatic identification of vehicles and other traffic factors is very important for which we need IoT technologies instead of using common image processing methods [44]. The intelligent traffic monitoring system will provide a good transportation experience by easing the congestion. It will provide features like theft-detection, reporting of traffic accidents, less environmental pollution. The roads of this smart city will give diversions with climatic changes or unexpected traffic jams due to which driving and walking routes will be optimized [1]. The traffic lighting system will be weather adaptive to save energy. Availability of parking spaces throughout the city will be accessible by everyone.

5.0.2 Smart Environment. Prediction of natural disasters such as flood, fire, earthquakes etc will be possible due to innovative technologies of IoT. There will be a proper monitoring of air pollution in the environment.

5.0.3 Smart Home. IoT will also provide DIY solutions for Home Automation with which we will be able to remotely control our appliances as per our needs. Proper monitoring of utility meters, energy and water supply will help saving resources and detecting unexpected overloading, water leaks etc. There will be proper encroachment detection system which will prevent burglaries. Gardening sensors will be able to measure the light, humidity, temperature, moisture and other gardening vitals, as well as it will water the plants according to their needs.

5.0.4 Smart Hospitals. Hospitals will be equipped with smart flexible wearable embedded with RFID tags which will be given to the patients on arrivals, through which not just doctors but nurses will also be able to monitor heart rate, blood pressure, temperature and other conditions of patients inside or outside the premises of hospital [45]. There are many medical emergencies such as cardiac arrest but ambulances take some time to reach patient, Drone Ambulances are already in the market which can fly to the scene with the emergency kit so due to proper monitoring, doctors will be able to track the patients and can send in the drone to provide quick medical care until the ambulance arrive.

5.0.5 Smart Agriculture. It will monitor Soil nutrition, Light, Humidity etc and improve the green housing experience by automatic adjustment of temperature to maximize the production. Accurate watering and fertilization will help improving the water quality and saving the fertilizers respectively [46].

5.0.6 Smart Retailing and Supply-chain Management. IoT with RFID provides many advantages to retailers. With RFID equipped products, a retailer can easily track the stocks and detect shoplifting. It can keep a track of all the items in a store and to prevent them from going out-of-stock, it places an order automatically. Moreover the retailer can even generate the sales chart and graphs for effective strategies.

6. SECURITY AND PRIVACY CHALLENGES

IoT makes every thing and person locatable and addressable which will make our lives much easier than before; however without a lack of confidence about the security and privacy of the user's data, it's more unlikely to be adopted by many [47]. So for its ubiquitous adoption, IoT must have a strong security infrastructure. Some of the possible IoT related issues are as followed:

6.1 Unauthorized Access to RFID

An unauthorized access to tags that contains the identification data is a major issue of IoT which can expose any kind of confidential information about the user so it needs to be addressed. Not just the tag can be read by a miscreant reader but it can even be modified or possibly be damaged. In this context, [47] summarized some of the real life threats of RFID which includes RFID Virus, Side Channel Attack with a cell-phone and SpeedPass Hack.

6.2 Sensor-Nodes Security Breach

WSNs are vulnerable to several types of attacks because sensor nodes are the part of a bi-directional sensor network as discussed in Section 4.2, which means other than the transmission of data, acquisition of data is also possible. [48] described some of the possible attacks that includes Jamming, tampering, Sybil, Flooding and some other kinds of attacks, which are summarized as followed:

- (1) Jamming obstructs the entire network by interfering with the frequencies of sensor nodes.
- (2) Tampering is the form of attack in which the node data can be extracted or altered by the attacker to make a controllable node.
- (3) Sybil attack claims multiple pseudonymous identities for a node which gives it a big influence.
- (4) Flooding is a kind of a DOS attack caused by a large amount of traffic that results in memory exhaustion.

6.3 Cloud Computing Abuse

Cloud Computing is a big network of converged servers which allow sharing of resources between each other. These shared resources can face a lot of security threats like Man-in-the-middle attack (MITM), Phishing etc. Steps must be taken to ensure the complete security of the clouding platform [49]. Cloud Security Alliance (CSA) proposed some possible threats among which few are Malicious Insider, Data Loss, Accounts Hijacking and Monstrous use of Shared Computers etc [50] which are summarized as followed:

- (1) Malicious Insider is a threat that someone from the inside who have an access to the user's data could be involved in data manipulating.
- (2) Data Loss is a threat in which any miscreant user who has an unauthorized access to the network can modify or delete the existing data.
- (3) Man-in-the-middle (MITM) is a kind of Account Hijacking threat in which the attacker can alter or intercept messages in the communication between two parties.
- (4) Cloud computing could be used in a monstrous ways because if the attacker gets to upload any malicious software in the server e.g. using a zombie-army (botnet), it could get the attacker a control of many other connected devices.

7. CONCLUSION

With the incessant burgeoning of the emerging IoT technologies, the concept of Internet of Things will soon be inexorably developing on a very large scale. This emerging paradigm of networking will influence every part of our lives ranging from the automated houses to smart health and environment monitoring by embedding intelligence into the objects around us. In this paper we discussed the vision of IoT and presented a well-defined architecture for its deployment. Then we highlighted various enabling technologies and few of the related security threats. And finally we discussed a number of applications resulting from the IoT that are expected to facilitate us in our daily lives. Researches are already being carried out for its wide range adoption, however without addressing the challenges in its development and providing confidentiality of the privacy and security to the user, it's highly unlikely for it to be an omni-present technology. The deployment of IoT requires strenuous efforts to tackle and present solutions for its security and privacy threats.

8. REFERENCES

- [1] Rafiullah Khan, Sarmad Ullah Khan, Rifaqat Zaheer and Shahid Khan, "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," in *Proceedings of Frontiers of Information Technology (FIT)*, 2012, pp. 257-260
- [2] Guicheng Shen and Bingwu Liu, "The visions, technologies, applications and security issues of Internet of Things," in *E-Business and E-Government (ICEE)*, 2011, pp. 1-4
- [3] Ling-yuan Zeng, "A Security Framework for Internet of Things Based on 4G Communication," in *Computer Science and Network Technology (ICCSNT)*, 2012, pp. 1715-1718
- [4] "The "Only" Coke Machine on the Internet," *Carnegie Mellon University, School of Computer Science*.
- [5] M. Weiser, "The computer for the 21st century", *Sci. Amer.*, 1991, pp.66 -75

- [6] Jason Pontin, "Bill Joy's Six Webs," *MIT Technology Review*, 29 September 2005
- [7] Kevin Ashton, "That 'Internet of Things' Thing", *RFID Journal*, 22 June 2009
- [8] H.D. Ma, "Internet of things: Objectives and scientific challenge," in *Journal of Computer Science and Technology*, 2011, pp. 919-924
- [9] Nich Heath, "What the Internet of Things means for you". It can be accessed at:
<http://www.techrepublic.com/blog/european-technology/what-the-internet-of-things-means-for-you>
- [10] "Twine" by Supermechanical. It can be accessed at:
<http://supermechanical.com/twine>
- [11] De-Li Yang, Feng Liu and Yi-Duo Liang, "A Survey of the Internet of Things", in *International Conference on E-Business Intelligence (ICEBI)*, 2010
- [12] Bob Violino, "Top IT Vendors reveal their IOT strategies". It can be accessed at:
<http://www.networkworld.com/article/2604766/internet-of-things/top-it-vendors-reveal-their-iot-strategies.html>
- [13] Harald Sundmaecker, Patrick Guillemin, Peter Friess, Sylvie Woelffl, "Vision and challenges for realising the Internet of Things," *Publications Office of the European Union*, 2010
- [14] Gartner, Inc. It can be accessed at:
<http://www.gartner.com/newsroom/id/2905717>
- [15] "From the ARPANET to the Internet" by Ronda Hauben - TCP Digest (UUCP). Retrieved 2007-07-05
It can be accessed at:
<http://www.columbia.edu/~rh120/other/tcpdigest-paper.txt>
- [16] Jian An, Xiao-Lin Gui, Xin He, "Study on the Architecture and Key Technologies for Internet of Things," in *Advances in Biomedical Engineering*, Vol.11, *IERI-2012*, pp. 329-335
- [17] Lan Li, "Study of Security Architecture in the Internet of Things," in *Measurement, Information and Control (MIC)*, 2012, Volume: 1, pp. 374-377
- [18] "The Internet of Things," *ITU Report*, Nov 2005
- [19] Wang Chen, "AN IBE BASED SECURITY SCHEME OF INTERNET OF THINGS," in *Cloud Computing and Intelligent Systems (CCIS)*, 2012, pp. 1046, 1049
- [20] Hui Suo, Jiafu Wan, Caifeng Zou, Jianqi Liu, "Security in the Internet of Things: A Review," in *Computer Science and Electronics Engineering (ICCSEE)*, 2012, pp. 648-651
- [21] Miao Wu, Ting-lie Lu, Fei-Yang Ling, ling Sun, Hui-Ying Du, "Research on the architecture of Internet of things," in *Advanced Computer Theory and Engineering (ICACTE)*, 2010, pp. 484-487
- [22] Xu Cheng, Minghui Zhang, Fuquan Sun, "Architecture of internet of things and its key technology integration based-on RFID," in *Fifth International Symposium on Computational Intelligence and Design*, pp. 294-297, 2012
- [23] Debasis Bandyopadhyay, Jaydip Sen, "Internet of Things - Applications and Challenges in Technology and Standardization" in *Wireless Personal Communications*, Volume 58, Issue 1, pp. 49-69
- [24] Ying Zhang, "Technology Framework of the Internet of THings and Its Application," in *Electrical and Control Engineering (ICECE)*, 2011, pp. 4109-4112
- [25] Benjamin Khoo, "RFID as an Enabler of the Internet of Things: Issues of Security and Privacy," in *Internet of Things (iThings/CPSCOM)*, 2011, pp. 709-712
- [26] L.Atzori, A.Iera, G. Morabito, "The Internet of Things: A survey," in *Computer Networks - Science Direct*
- [27] H. Zhang, L. Zhu, "Internet of Things: Key technology, architecture and challenging problems", in *Computer Science and Automation Engineering (CSAE)*, 2011, Volume: 4, pp. 507-512
- [28] L.G. Guo, Y.R. Huang, J. Cai, L.G. QU, "Investigation of Architecture, Key Technology and Application Strategy for the Internet of Things," in *Cross Strait Quad-Regional Radio Science and Wireless Technology Conference (CSQRWC)*, 2011, Volume: 2, pp. 1196-1199
- [29] Sohraby, K., Minoli, D., Znati, T. "Wireless sensor networks: technology, protocols, and applications", *John Wiley and Sons*, 2007 ISBN 978-0-471-74300-2, pp. 15-18
- [30] "WISP" by Intel Labs; It can be accessed at:
<http://wisp.wikispaces.com>
- [31] E. M. Tapia, S. S. Intille, and K. Larson, "Portable wireless sensors for object usage sensing in the home: Challenges and practicalities," in *Proceedings of the European Ambient Intelligence Conference. vol. LNCS 4794 Berlin Heidelberg: Springer-Verlag 2007*
- [32] IEEE 802.15 WPAN Task Group 4.
It can be accessed at:
<http://www.ieee802.org/15/pub/TG4.html>
- [33] G. Montenegro, N. Kushalnagar, J. Hui, D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks"
- [34] R. Roman, C. Alcaraz, J.Lopez, N. Sklavos, "Key Management Systems for Sensor Networks in the Context of the Internet of Things," *Computers & Electrical Engineering*, Volume: 37, Issue: 2, 2011, pp. 147-159
- [35] B.B.P. Rao, P.Saluia, N.Sharma, A.Mittal, S.V.Sharma, "Cloud computing for Internet of Things & sensing based applications," in *Sensing Technology (ICST)*, 2012 *Sixth International Conference*, IEEE
- [36] X.Xiaohui, "Study on Security Problems and Key Technologies of The Internet of Things," *Computational and Information Sciences (ICCIS)*, 2013, pp. 407-410
- [37] O.Vermesan, P.Friess, "Internet of Things ? From Research and Innovation to Market Deployment," *River Publishers*, pp. 74-75
- [38] I.Akyildiz and J.Jornet, "THE INTERNET OF NANO-THINGS," *IEEE Wireless Communications*, Volume: 17 Issue: 6, 2010, pp. 58-63
- [39] V.M. Lubecke, Jung-Chih Chiao, "MEMS technologies for enabling high frequency communications circuits," in *Telecommunications in Modern Satellite, Cable and Broadcasting Services*, 1999, Volume: 2, pp. 382-389
- [40] "Cisco 40 Gigabit Module". It can be accessed at:
<http://www.cisco.com/c/en/us/products/interfaces-modules/40-gigabit-modules/index.html>
- [41] R. Abdmeziem, D.Tandjaoui, "Internet of Things: Concept, Building blocks, Applications and Challenges, *Computers and Society, Cornell University*"
- [42] "What we're driving at," Google Official Blog.
It can be accessed at:
<http://googleblog.blogspot.com/2010/10/what-were-driving-at.html>

- [43] [Y.Cao, W.Li, J.Zhang, "Real-time traffic information collecting and monitoring system based on the internet of things," in *Pervasive Computing and Applications \(ICPCA\), 2011 6th International Conference*, pp. 45-49](#)
- [44] [L.Xiao, Z.Wang, "Internet of Things: A New Application for Intelligent Traffic Monitoring System," in *JOURNAL OF NETWORKS, 2011*](#)
- [45] [P.Fuhrer, D.Guinard, "Building a Smart Hospital using RFID technologies,"](#)
- [46] [F.TongKe, "Smart Agriculture Based on Cloud Computing and IoT," in *Journal of Convergence Information Technology \(JCIT\), Jan'13*](#)
- [47] "RFID Security Issues - Generation2 Security".
It can be accessed at:
<http://www.thingmagic.com/index.php/rfid-security-issues>
- [48] [Y.Wang, G.Attebury And B.Ramamurthy, "A Survey on Security Issues in Wireless Sensor Networks," in *IEEE communications Survey and Tutorials, 2nd Quarter 2006*.](#)
- [49] [M.Aamir, Prof. X.Hong, A.A.Wagan, M.Tahir, M.Asif, "Cloud Computing Security Challenges and their Compromised Attributes," in *International Journal of Scientific Engineering and Technology*, Volume 3, Issue 4, pp. 395-399](#)
- [50] [V. Ashktorab, S.R.Taghizadeh, "Security Threats and Countermeasures in Cloud Computing," in *International Journal of Application or Innovation in Engineering and Management \(IJAIEEM\)*, Volume 1, Issue 2, Oct' 12.](#)