INTERNET OF THINGS - REVIEW, CHALLENGES AND RECOMMENDATIONS

Mohd Umar John[1], Junaid Latief Shah2, Gazi Imtiyaz3, Gazi-ul-Islam4
Research Scholar Shri Venketeshwara University UP [1,4]
Assistant Professor SP College Srinagar [2,3]

ABSTRACT

The IoT (Internet of Things) with a vast network area has created diverse number of opportunities for achieving desirable change by the people connected within a society and has made sustainable technological development in the present scenario. IoT technologies include the use of RFID's, WSN, EPC, actuators and protocols such as IP protocol, bluetooth and zigbee. The main characteristic feature of IoT is support for heterogeneous and interoperability functions. In this paper, we lay emphasis on IoT technology highlighting its objectives and applications. The paper also presents IoT layered architecture with its main focus on privacy and security issues. Further, paper also presents challenges and open issues that need to be discussed including recommendations for future research in this area.

Keywords: IoT, RFID, EPC, WSN, IP

Introduction

The term Internet of Things (IoT, also known as the Internet of Objects) was first coined by Kevin and refers to the network of connected everyday objects. It is commonly referred as a self-configuring wireless network of sensors with purpose of interconnecting of all objects. The concept of IoT is an attribute of MIT Auto-ID Center, founded in 1999.At MIT, David Brock was first to mention about Internet of Things in his Auto-ID center paper about the Electronic Product Code in 2001 (ashton,2009; brock,2001). Global Standards Initiative on Internet of Things (IoT-GSI) termed it as a global infrastructure for the information society in 2013 because more than 16 billion people are connected using this technology (patrick et al ,2013). The IoT will create numerous opportunities to make desirable change in human life style. The IoT serves as a base that is rapidly gaining popularity in the field of modern wireless telecommunication system (haller et al ,2008). The primary idea of IoT shows the presence of variety of things or objects covering us, such as Radio-Frequency Identification (RFID) tags, sensors, actuators, mobile phones, etc. and communicating with us by unique addressing schemes, to attain basic goals. The primary strength of the IoT system is its tremendous impact on several aspects of human behavior in everyday life. IoT has effective and beneficial impact on human life style that necessitated US National Intelligence Council to incorporate IoT in its list of six disruptive civil technologies (nic,2008). From the technological perspective, IoT must have following three characteristics (shanzhi et al, 2014).

a. Comprehensive Perception:
It includes the use of RFID (Radio Frequency Identification), sensors and multidimensional barcodes and acts as new technology to obtain information about the anywhere location of object. It can make

information and communication system invisibly embedded in the surrounding environment. People can easily interact remotely with each other by means of a sensor network.

b. Reliable Transmission:
IoT objects are made available by means of varied resources including radio-network technology like tele-communication and internet. Telecommunication technology includes different wired and wireless transmissions, switching, networking and gateway methods. Interactive and healthy interaction can be created easily with the physical, virtual and digital world by means of M2M (Machine to Machine) and H2M (Human to Machine) interactions.

c. Intelligent Processing:
Creating a large database for storage of IoT data involves inherent support from intelligent computing technologies and its applications. The intelligent processing is also required for processing billions of objects instantly by means of cloud computing technology.
Although IoT has made human life easy and comfortable in a connected approach but it has critical issues related with its architecture, security and privacy which need to be addressed so as to provide a solution for the lifelong survival of this technology (takabi et al,2010; chen et al,2012; mcdaniel et al, 2009). IoT faces several critical issues and challenges regarding security and privacy which includes

Å Management of heterogeneous devices and their scalability.
Å Networked knowledge and context.
Å Emergence of new set of network protocols and architecture.
Å Problems with authentication and data integrity.
Å Privacy issues related with data processing, connected devices, and information exchange.
Å Lack of uniform standard architecture for IoT.
Å Quality of Service issues in IoT.
Å Ethical issues.

This paper surveys IoT with respect to its architecture and related issues. The paper discusses applications and as well as objectives of IoT. Focus will be on discussing the security and privacy issues including their proposed and feasible solutions from the existing literature. The paper also highlights challenges towards implementation of IoT in different technological aspects. Further we highlight some open issues including future scope of IoT technology.

1. Objectives of IoT

As compared to traditional information network, IoT objectives are based on advancement in information communication technology which include current scenario of customer / user demands. The objectives of IoT are generally divided into three categories (riahi et al. 2013; ma,2011).

a. Extensive Interconnection
The interconnection capabilities of IoT have been extended to interconnect with all intelligent or non-intelligent information sources /objects. These make IoT capable of handling and interconnecting billions

of devices that include sensors, actuators, vehicles and RFID devices. The IoT connected devices are powered directly from the batteries. Also, the computational abilities of these connected devices vary from one another. The mode of interconnection of these devices can be wired or wireless. Also, communication mode includes single or multi-hop communications with strong or weak state of Routing. A highly interconnected network element is therefore required for efficient and intelligent heterogeneous networks.

b. Intensive Information Perception
IoT has achieved the global environment awareness by paradigm of collaboration between multiple sensor systems. Earlier, there were certain critical issues related to single sensor objects. The aspects of criticalities include inconsistent information that is caused due to distortion of space time mapping. This also includes non-uniformity among different data types. The number of inaccuracies in data is caused by different sampling methods and sensors with different abilities. Information discontinuation is also caused by the dynamic network transmission capabilities. Another criticality includes incomplete sensing of information which may cause incomprehensiveness of data/information. Also, dynamic network of IoT may lead to partial loss of data/ information.

c. Comprehensive Intelligent Service
IoT can provide comprehensive intelligent services of physical world objects that are actively involved in it. Different intelligent networks when integrated provide dynamic intelligent services such as weather condition reporting, environment and health conditions and thus achieve the harmony of people as well as of physical objects required for civilized connected society. IoTôs comprehensive intelligent services need change for dynamic environment for adaptation to latest developing software, service delivery mechanism and also methods that provide flexibility in intelligent service system.

2. Architecture of IoT

As IoT is a very diverse concept, as such it does not have any uniform architecture. The general framework of IoT architecture must consist of sensors, network, communications and different computing technologies. Different models of IoT architecture have been proposed over a period of time by well known researchers. Among the most reliable and suited one is the ITU Architecture (agrawal et al,2011).

4.1 ITU Architecture

As per the assessment and recommendation of International Telecommunication Union (ITU), the architecture of IoT consists of five (5) layers which are analogous to OSI reference Model. The five-layered architecture of IoT as shown in figure 1 consists of the following layers.

The Sensing Layer/ Physical Layer
This layer is also known as perception or device layer and consists of physical objects including sensor devices. It basically deals with the identification and collection of information of a specified object. The sensors used are object information specific which include RFID, multidimensional barcode readers or infrared sensors which record information on the basis of location, temperature, motion, orientation,

changes in composition of air etc. The information collected by the objects is then passed to the access/ data link layer for further processing.

The Access / Data Link Layer
This layer works in coordination with the sensing /physical layer as the information is collected using underlying connected sensor hardware. Usually UART devices are used. Also, this layer facilitates communication between the sensors and controllers and also acts as an interface using MAC/IP addresses for sockets.

The Network Layer
The network layer is also referred to as transmission layer. The information collected passes from the access layer to the network layer for onward secure transfer to information processing system. The medium of information transfer can be both wired as well as wireless. The wireless technology includes 4G/3G, UTMS, Wi-Fi, Bluetooth, Zig-Bee etc.

The Middleware /Transport Layer
The middleware layer functions as the service management and is responsible for device mapping for same service types. It also provides the dedicated link to the database for data storage. This layer performs information processing and ubiquitous computations with automatic decision making based on results.

The Application/Data Layers
This performs global function of management of applications based on the objects traced and processed in the middleware. This is the layer where user actually interacts with IoT and enjoys its variety of services. This layer has another sub-layer called Business Application layer used for business purposes and that is why many researchers or authors have listed it as 6th layer of IoT architecture.

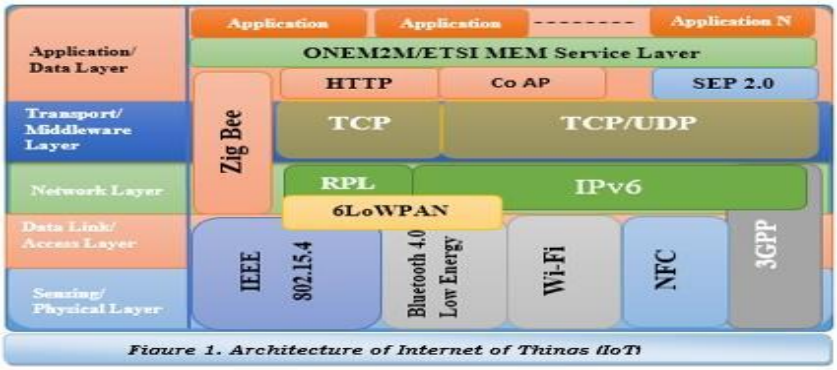

Figure 1: Five layered architecture of IoT

3. Security and Privacy Issues in IoT

IoT being the evolving technology faces major and critical challenges with respect to its security. The layered architecture must be equipped with security framework at every layer in order to avoid

vulnerabilities. Security of entire IoT system involves the series of properties like confidentiality, integrity, authentication, authorization etc.

IoT has several major security implications because of its changing hardware components at its general layered architecture. Generally, IoT devices work on the battery power and low power devices have low clocked CPUs with low clock rates. Therefore, energy computation for cryptographic algorithms is expensive and low power CPUs cannot support fast computation required for the algorithms directly (takabi et al ,2010). Also, devices that constitute IoT have limited primary memory and secondary flash memory as compared to traditional computing systems. The IoT devices are equipped with Real Time Operating System (RTOS)/ low weighted General-Purpose Operating Systems (GPOS) and are operated using system softwareôs and their associated service applications. Therefore, security must obviously be memory efficient. Though devices in IoT are efficient in terms of memory but does not support the traditional/conventional security algorithms because of issues with RAM and hard disk. These issues might create further memory issues after booting up of the systems (mcdaniel et al, 2009; arampatzis et al, 2005). The IoT devices in remote areas remain unattended for most of the time and there are chances of an attack / intrusion. As such, data may be tampered easily and therefore tamper resistant packaging is the prime need of the hour (arampatzis et al. 2005)

The software part of the IoT also faces several critical issues. The operating system embedded within IoT devices have weak network protocol stack and may not have enough security modules inviting probability for faults. For this purpose, fault tolerant and robust protocol needs to be developed (mcdaniel et al, 2009). Another issue is that operating system embedded with the IoT devices and protocol might not support the new code for remote programming

Another important domain of IoT is the network which also faces some security issues. IoT network mobility is an important attribute of IoT which supports number of devices for communication without being pre-configured and for this issue, development of security algorithms is the prime priority (mcdaniel et al, 2009; arampatzis et al. 2005) Since the familiarity of IoT is increasing day by day and therefore number of devices also get increased with the global information network. The current IoT network cannot be handled by security scheme and needs to b re-engineered. The vast network of IoT has diversity of devices ranging from small smart phone to personal computer systems. It is therefore very difficult to design a single security scheme for such vast and big networks. Since the communication media in IoT network can be both wired as well as wireless, therefore both the communication media must be equipped with the comprehensive security protocol which is very difficult task. The traditional security schemes are unsuitable for IoT network because of multiple protocols. The IoT has a dynamic topology because the devices in it may leave the network at any time and new devices may get connected. The current model of security does not support these topological changes and is not suitable for the smart network device security (takabi et al ,2010).

From the above discussion, it is concluded that precautions and preventive measure must be followed while designing the security solutions for IoT devices. The chief and important measures are that are expected to encounter by the IoT security scheme are:

- Data integrity in IoT is one of important security measure and must be maintained so to avoid tempering of data.

- Protection of data/ information in IoT is another preventive measure that keeps information confidential and is stored strictly.
- There must be data abstraction or anonymity in case of the source data due to which, the confidentiality and privacy remains maintained in IoT.
- The access level security enables IoT devices to ensure the identity. Users are required to prove their entity for validation purpose and for performing the network administrative tasks for controlling IoT devices.
- IoT must ensure authentication for access to service node by the help of well-developed and strong access control mechanism.
- The whole network of IoT and associated devices must have robustness so that if any kind of drastic or anomalous situation arises, it must continue work and keep the network alive.
- For the survival of IoT, it must have a mechanism of providing limited services in case of power loss failure.
- IoT must have secure bootstrapping mechanisms for data processing before network is made functional. It must also support the secure data transmission with well-defined and proper cryptographic algorithms.

Privacy is another issue with IoT enabled devices. The privacy is described by the abstraction of personal data and control mechanism for maintaining the data reliability. It is considered to be basic and fundamental right and provide the highest degree of reliable information. Though the privacy mechanism is very difficult in such a vast network but technological improvement in the field has made it possible by providing number of suitable technologies called privacy enhancement technologies (PET) (kumar et al ,2014). Some of the PET technologies include Private Information Retrieval System (PIR), DNS security extensions (DNS-sec), Onion Routing, Transport Layer Security (TLS) and Virtual Private Network (VPN).

4. Applications of IoT

IoT is a diverse concept of technological suite in which different technologies are mapped to achieve the specific goals. It finds application in every aspect of our life which we encounter. The applications of IoT have been divided in three different domains i.e. society, industry and environment. Every domain has specific set of activities and cannot be separated. Thus, the applications and services rendered by IoT are inter and intra-domain (chen et al ,2014; argrawal et al ,2011).

One of the applications of IoT is Natural Disaster Prediction. The sensor technology in IoT has an autonomous coordination. The simulation helps to predict the land-slide occurrences and other natural disasters and hence necessary appropriate actions can be taken in advance for the welfare of the society (chen et al ,2014).

IoT also find their usability in Industrial applications during different kinds of operations. IoT sensor technology is used in automobile vehicles to make them more interactive and secure (argrawal et al ,2011). Environmental performance and data processing is also determined by IoT technology. It allows the secure

monitoring of industrial plant to reduce the accidental instances and real-time vehicle diagnosis (chen et al ,2014).

The popularity and usability IoT finds its application in the academia also. Using IoT academic operation can be made more interactive and result oriented. It can even be used as a tool for live smart class (kumar et al,2014). It can be used to monitor and detect unfavorable circumstances and intervening environmental variable so that the necessary and proper action and preventive measures are taken.

IoT technology is also used for monitoring different water levels by the help of network sensors with relevant simulation techniques for long term water intervention of catchment area management (arampatzis et al, 2005; kumar el al,2014) Alerts can be given to users of water streams for water scarcity and also alert for dangerous implications can be issued.

IoT serves as the lifesaving technology in medical applications. The sensors of IoT can monitor the different parameters of patients like heartbeat; blood pressure etc. so that a complete record is maintained and proper treatment is applied to patients (chen et al ,2014; argrawal et al ,2011). This technology is very useful and lifesaving during emergencies and causalities because the critical conditions of the patients are discussed by different experts across the world and at the same time best real time possible treatment is provided.

With advancement of technology, the people in the world became more civilized and smart home itself is a sign of smart civilization. The smart homes are designed by the IoT sensor technology due to which, energy consumption management becomes easy. The IoT sensor network technology makes the homes smart in terms security, emergency detection, object tracing within homes and also in terms of instructiveness (argrawal et al ,2011).

The concept of smart city is possible only with IoT sensor network technology (chen et al ,2014; argrawal et al ,2011). because it has the capability to detect or monitor the quality of air, discovering emergency routes, effective lighting of the cities and also monitoring of the water quality. In addition to above IoT find their applications in design of smart security, smart transport system design, designs of border security and military application, weather forecasting application etc.

5. Open Issues and Challenges

The success of IoT technology is evident by its unlimited applications and its potentialities with its gaining popularity. Unfortunately, it also encounters number of issues and challenges. The first challenge is regarding infrastructure. The unique framework of IoT is commonly expected to provide integrated developmental solution for future purpose (tsai el al,2017). General communication interface is said to be the alternative solution that provide the flexible service for data exchange. Being presence of properties of decentralization and heterogeneity still has impact on design of IoT, because the developmental design of IoT must be compatible with the existing systems and technologies (chen et al,2014; ma,2011) Another factor is computational intelligence. Since data is managed efficiently in IoT and demand for smart and intelligent decision-making system is under consideration, the data mining and other intelligence technologies are still at their early developmental stage and for this, the computational intelligence technologies are applied to provide better service (chen et al ,2014; ma ,2011; tsai el al,2017). The data extraction in IoT for any developer is also a prime concern and needs to be addressed. The process of data extraction has severe impact on the performance of IoT system particular in the heterogenic environment

and for re-engineering the whole memory size, computation power and network bandwidth are taken in to consideration (shanzhi et al,2014; miorandi et al,2012; borgia et al,2014; tsai et al,2014).

The integration of unlimited resources of computing and large storage capacity of cloud computing with the existing IoT is an important open issue which needs to be addressed. IoT is a suite of different wide range technologies with large number of smart interconnected devices and sensors that are sometimes invisible, transparent and nonintrusive (chen et al ,2014). The communication between these devices generally occurs in the wireless mode, autonomic and adhoc manner and services supported by it are more complex and decentralized. The data integration and interaction adaptation by these smart devices and the information sensed have several uncertainties (ma,2011). The data exchange of large scale network of heterogeneous components is the main characteristic feature of IoT and it supports the strong dynamic autonomy. Thus, interconnection and interoperability need to be improved for the efficient dynamic autonomy (chen et al ,2014).

In terms of security and privacy, there are large numbers of connected objects in IoT expanded over geographic area which need to be protected from intrusion (khan et al ,2012) There is a need for low cast and M2M oriented technical solution for the guaranteed security and privacy in contrast with the traditional network systems (chen et al ,2014). Since public key cryptosystem benefits from authentication scheme design, but lack of global root certification authority may hinder number of such schemes actually being deployed and in a huge network like IoT, it is a challenge to issue certificate for objects (zhang et al,2014). The cryptographic key management is an important constraint in security mechanism which is a difficult aspect of cryptography (zhang et al,2014). The light-weighted cryptographic algorithms with high performance sensors must be applied for coping up with security issues (suo et al ,2012) and therefore the public key cryptosystems and complex security protocols is the key challenge of IoT security.

6. Conclusion

In this paper, the concept and background IoT is presented with corresponding characteristics and objectives. The paper presents outline of the research and work that has already been carried out. The paper surveys the detailed layered architecture and associated technologies of IoT. In this paper, we also provide detailed overview of applications of IoT and a special attempt has been made for analyzing the security and privacy issues including requirements. Lastly, an attempt has been made to discuss open issues and challenges with respect to IoT security and privacy.

Since IoT is still evolving while making remarkable change in our lifestyle, still there are several areas that are emerging subjects for further research. Prominent issues that must be taken into consideration include systematic approach for the inter-operability of devices at different services layers, cross layer collaborations, real time data handling, development of intelligent systems for a fast and reliable IoT network and data Transparency in IoT.

References

"I could be wrong, but I'm fairly sure the phrase ôInternet of Thingsô started life as the title of a presentation I made at Procter & Gamble (P&G) in 1999", Kevin Ashton, RFID Journal, 22 June 2009.

Agrawal, Sarita, and Manik Lal Das. "Internet of Thingsð A paradigm shifts of future Internet applications." Engineering (NUiCONE), 2011 Nirma University International Conference on. IEEE, 2011.

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.

Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." Computer networks 54.15 (2010): 2787-2805.

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

Borgia, Eleonora. "The Internet of Things vision: Key features, applications and open issues." Computer Communications 54 (2014): 1-31.

Chen, Deyan, and Hong Zhao. "Data security and privacy protection issues in cloud computing." Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on. Vol. 1. IEEE, 2012.

Chen, Shanzhi, et al. "A vision of IoT: Applications, challenges, and opportunities with china perspective." IEEE Internet of Things journal 1.4 (2014): 349-359.

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

Chorost, M. (2008) The Networked Pill, MIT Technology Review, March.

David L. Brock, MIT Auto-ID Center, MIT-AUTOID-WH-002, "The Electronic Product Code", January 2001.

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

Gubbi, Jayavardhana, et al. "Internet of Things (IoT): A vision, architectural elements, and future directions." Future generation computer systems 29.7 (2013): 1645-1660.

Guillemin, Patrick, et al. "Internet of Things Standardisation Status, Requirements, Initiatives and Organisations." RIVER PUBLISHERS SERIES IN COMMUNICATIONS (2013): 259.

Haller, Stephan, Stamatis Karnouskos, and Christoph Schroth. "The internet of things in an enterprise context." Future Internet Symposium. Springer, Berlin, Heidelberg, 2008.

Hossain, Md Mahmud, Maziar Fotouhi, and Ragib Hasan. "Towards an analysis of security issues, challenges, and open problems in the internet of things." *Services (SERVICES), 2015 IEEE World Congress on*. IEEE, 2015.

Khan, Rafiullah, et al. "Future internet: the internet of things architecture, possible applications and key challenges." Frontiers of Information Technology (FIT), 2012 10th International Conference on. IEEE, 2012.

Kumar, J. Sathish, and Dhiren R. Patel. "A survey on internet of things: Security and privacy issues." International Journal of Computer Applications 90.11 (2014).

Li, B.A. and Yu, J.J. (2011) Research and Application on the Smart Home Based on Component Technologies and Internetof Things. Procedia Engineering, 15, 2087-2092. http://dx.doi.org/10.1016/j.proeng.2011.08.390.

Ma HD. Internet of things: Objectives and scientific challenges. JOURNAL OF COMPUTER SCIENCE AND TECH-NOLOGY 26(6): 919{924 Nov. 2011. DOI 10.1007/s11390-011-1189-5.

Madakam, Somayya, R. Ramaswamy, and Siddharth Tripathi. "Internet of Things (IoT): A literature review." Journal of Computer and Communications3.05 (2015): 164.

Madsen, Henrik, et al. "Reliability in the utility computing era: Towards reliable fog computing." Systems, Signals and Image Processing (IWSSIP), 2013 20th International Conference on. IEEE, 2013.

McDaniel, Patrick, and Stephen McLaughlin. "Security and privacy challenges in the smart grid." IEEE Security & Privacy 7.3 (2009).

Miorandi, Daniele, et al. "Internet of things: Vision, applications and research challenges." Ad Hoc Networks 10.7 (2012): 1497-1516.

Moeinfar, D., Shamsi, H. and Nafar, F. (2012) Design and Implementation of a Low Power Active RFID for ContainerTracking @ 2.4 GHz Frequency: Scientific Research.

Nic, N. I. C. "Disruptive civil technologies: Six technologies with potential impacts on us interests out to 2025." Tech. Rep. (2008).

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.

Razzak, F. (2012) Spamming the Internet of Things: A Possibility and its probable Solution. Procedia ComputerScience, 10, 658-665. http://dx.doi.org/10.1016/j.procs.2012.06.084.

Riahi, Arbia, et al. "A systemic approach for IoT security." Distributed Computing in Sensor Systems (DCOSS), 2013 IEEE International Conference on. IEEE, 2013.

Sajid, Anam, Haider Abbas, and Kashif Saleem. "Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges." IEEE Access 4 (2016): 1375-1384.

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

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

Suo, Hui, et al. "Security in the internet of things: a review." Computer Science and Electronics Engineering (ICCSEE), 2012 international conference on. Vol. 3. IEEE, 2012.

Takabi, Hassan, James BD Joshi, and Gail-Joon Ahn. "Security and privacy challenges in cloud computing environments." IEEE Security & Privacy 8.6 (2010): 24-31.

Tsai, Chun-Wei, Chin-Feng Lai, and Athanasios V. Vasilakos. "Future Internet of Things: open issues and challenges." *Wireless Networks* 20.8 (2014): 2201-2217.

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

Zhang, Zhi-Kai, et al. "IoT security: ongoing challenges and research opportunities." Service-Oriented Computing and Applications (SOCA), 2014 IEEE 7th International Conference on. IEEE, 2014.