A Journal Publication of the Faculty of Science, Adeleke University, Ede, State of Osun, Nigeria
www.jasra.adelekeuniversity.edu.ng
Vol 3, 2016 Series

Internet of Things: Survey of the Security Challenges and Countermeasures

[1]Adegboye, M.A., [2]Olaniyan, O.M., [3]Ajao, L.A. [4]Okomba, N.S. & [5]Okwor, O.C.
[1,2,4,5]Department of Computer Engineering, Federal University Oye-Ekiti, Nigeria
[3]Department of Computer Engineering, Federal University of Technical Technology, Minna, Nigeria
mutiu.adegboye@fuoye.edu.ng,olatayo.olaniyan@fuoye.edu.ng,ajao.wale@futminna.edu.ng
[4]nnamdi.okomba@fuoye.edu.ng, [5]candidus.okwor@fuoye.edu.ng

ABSTRACT

The emphasis of this paper is to undertake a survey of Internet of Things, the security challenges and possible countermeasures. Internet of things interconnects objects, people, service and devices to communicate over the Internet. It finds application in different areas like transportation, healthcare, smart home and other areas that involve communication over the Internet in order to execute tasks intelligently, without human intervention. This is why it is very important to understand the security challenges associated with the internet of things and consider the possible countermeasures.

Keywords*:* Internet of Things; Network; IoTs Architecture; Privacy ; Security; Countermeasure

1. INTRODUCTION

Internet of things (IoTs) is an innovative area that is quickly gaining ground in the area of wireless communications (Li, Xiaoguang, Ke, & Ketai, 2011); (Daniel Giusto, Iera, Morabito, & Atzori, 2010); (Friess, 2013). The elementary concept of this idea is the presence of a collection of things such as sensor, mobile phone, radio frequency identification (RFID) etc. that are able to communicate others object to attain common goal via specific address system (D. Giusto, Lera, G., & Atzori, 2010). It has been envisaged that sooner than later, IoTs will grow to become a ubiquitous worldwide computing network that will link machine, people and everything to the internet (Khan, Khan, Zaheer, & Khan, 2012); (Vermesan et al., 2011). In IoTs everything is virtual (Roman, Najera, & Lopez, 2011), which means each person and things has a location, unique address and readable partner on the Internet (Atzori, Iera, & Morabito, 2014).

Owing to these characteristics, IoTs promise to expand anyhow to anywhere with any network at any time to compete with any services. Figure 1 illustrates how the IoTs allows people and things connect with anything at any time in anyplace. Upon all these numerous potential benefits, several noteworthy issues need to be addressed; among them is the security issue. The IoTs and its users can become vulnerable to malicious attacks (Borisov, Goldberg, & Wagner, 2001) and its widespread acceptance can also lead to the development of even more sophisticated attack models. To overcome such challenges, a proper understanding of the technology of IoTs and traditional security mechanisms such as lightweight cryptography, privacy assurance and secure protocol is required.

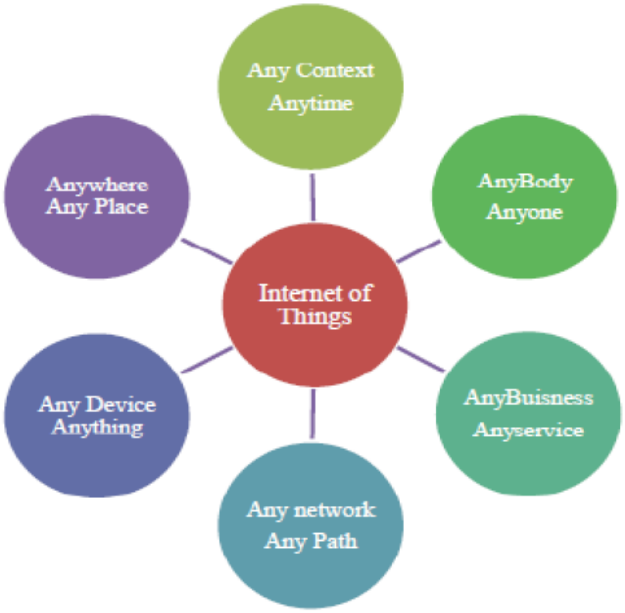

Figure 1: Graphical Representation of IoTs (Perera, Zaslavsky, Christen, & Georgakopoulos, 2013)

2. EVOLUTION OF IOTS

In 1999, the terms of IoTs originated from a man named Kevin Ashton from MIT. He was regarded as the first person to use the terms of IoTs in a presentation about RFID at Procter and Gamble in 1999 (Sinph, Pasqueier, Bacon, Ko, & Eyers, 2015), since then the word of IoTs becoming more popular in every present days. Before the evolution of IoTs, communication between two computers (network) made possible in late 1960s (Sproull & Kiesler, 1991). In the early of 1980s, TCP/IP stack brought to existence (Fall & Stevens, 2011); (Piscitello & Chapin, 1993); (Werle, 2001), follow by commercial use of the world wide web (WWW) in the1991 (Albert, Jeong, & Barabási, 1999); (Aghaei, Nematbakhsh, & Farsani, 2012); (Crossman, 1997) which made the internet more popular and attained prompt progression. After then mobile devices started connected to the internet. With emergence of social network users begin to communicate over the internet (Leiner et al., 2009), and immediately all these technologies was achieved the next emerge is the IoTs where object around us including machine to machine (m2m) started connected to communicate via RFID, Bluetooth, Internet and so on (Kumar & Patel, 2014). Figure 2 illustrates technology progression starting from network to the IoTs.

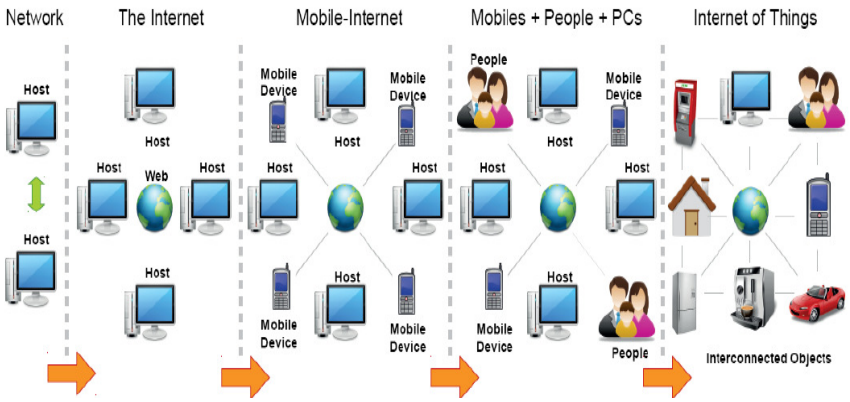

Figure 2: Evolution of Internet of Things (Perera, et al., 2013)

IoTs promise to reinvent a universe world where the entire smart object in our environment will be communicate with one and others over the internet with less/no human intervention. The essential goal is to build a healthier world for human beings where object in our environment can predict what we desired and take the action accordingly without specify instruction.

3. ARCHITECTURE OF Iots

In IoTs architecture, each of the layers is classified by its purpose and defined based on the devices that are operates within each of them. Although there are different view concerning the number of layer in IoTs, however, according to researchers (Zhao & Ge, 2013); (Leo, Battisti, Carli, & Neri, 2014), IoTs is operate mainly on three layer (Karagiannis, Broido, & Faloutsos, 2004) which are Application layer, Network layer and Perception layer. Each layer inherited security issue associated with it. Figure 3 shown architecture of internet of things and detail devices that are operating in each of the layer.

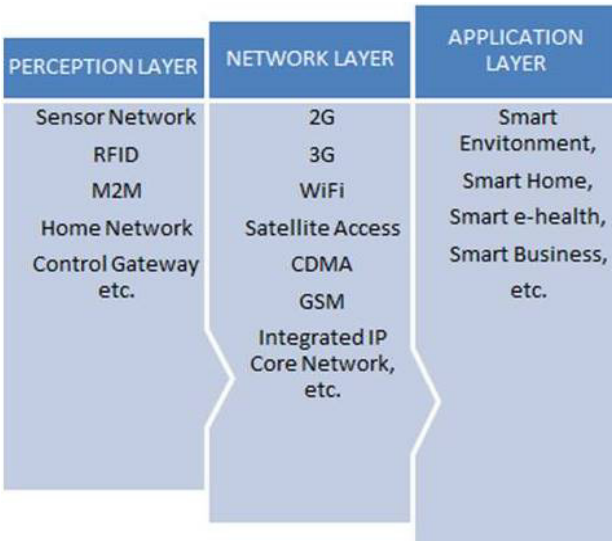

Figure 3: Architecture of IoTs

3.1 Perception Layer

Perception layer which is also called recognition/sensor layer obtain the environmental attribute through the uses of sensor. This layer senses, collect and process data or information obtains from sensor and then transfers it to the layer that performing data routing and transmission. The function of IoTs cooperation in local and short range networks can also perform in this layer (Atzori, Iera, Morabito, & Nitti, 2012).

3.2 Network Layer

The function of this layer is enabling Data routing and transmission to the various IoTs devices and hub over the internet. In this layer, gateways, switches, internet and routing devices operate through the uses of some of the modern technology such as 4G, Wifi, Zigbe, and 3G, to provide various network services (Leo, et al., 2014).

3.3 Application Layer

This layer securities the availability, confidentiality integrity and authenticity of the data. In this layer, the main function of IoTs is to ensure communication between machine, people and things is achieved (Atzori, et al., 2012).

3.4 Security Challenges in Each Layer

Each layer of IOTs is vulnerable to series of security threats and attack. These may be passive or active attacks, which may be created by external or internal network. Table 1 listed security concerns and threats at each of highlighted layer of IoTs (Abomhara & Køien, 2014).

TABLE 1:SECURITY CONCERNS AT EACH LAYER OF IOT

Layer	Security Concerns and Threats
Perception	physically attacks, Wireless communication capacity and vigorous IoTs topology
Network	Passive moniturng, analysis of traffict, eavesdropping, multifariousness protocols and network devices.
Application	Lack of standard and global confidence policies, validation mechanisms.

4. APPLICATION OF IOTS

In a research carried out by (Bing, Fu, Zhuo, & Yanlei, 2011) on IoTs project in 2010, they identified IoTs application scenarios and group it into fourteen classes including Smart home, Lifestyle, Agriculture, Transportation, Retail, Smart city, Smart factory, Emergency, Culture and tourism, Healthcare, Supply chain, Energy, User identification and Environmental. In this research, the concentration will limited to application of IoTs in smart home, healthcare and intelligent community system.

4.1 IoTs in Smart Home

Nowadays, smart home systems are becoming intellectualized and effective with continue growth and cost effective in electronic, information and communication technology. It interconnects through the internet with all others everyday objects and sensor for linking virtual and physical device. Figure 4 shown pictorial representations of IoTs smart home systems, with a motion sensor, security alarm and control systems.

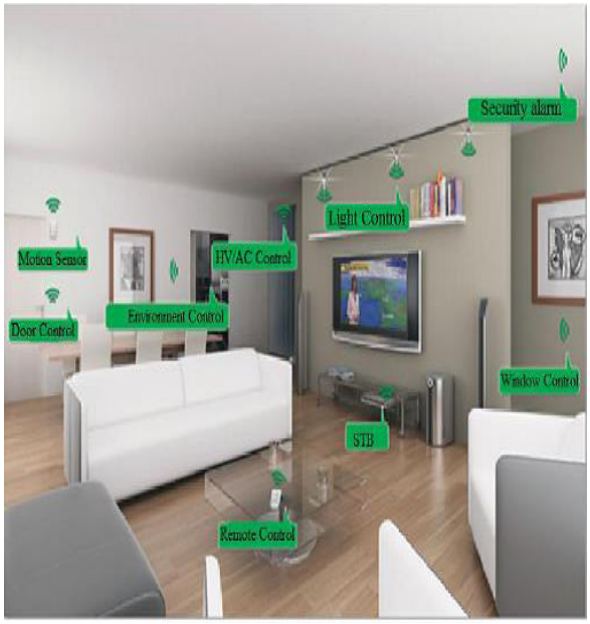

Figure 4: IoTs smart home system (Bing, et al., 2011)

From the above system, reading of the remote meters can be achieved, which means the data associated with intelligent home system, water, Air conditioning system, light and telecommunications can be send to their corresponding service automatically to know the condition of the house. Via the uses of intelligent home systems, home ventilation, windows, doors, air conditions system, light etc. can be remotely controlled.

4.2 IoTs in Healthcare

Owing to rapid growth in population, high rate of expansion in the rural community, social disequilibrium resources consumption, elderly population and some others social challenges that have becoming gradually seeming in the healthcare environment, IoTs was introducing to address some of these issues. Figure 5 shown the securing digitized campus clinical healthcare delivery system deployed to healthcare service Centre at the Federal University of Technology, Minna (FUTMINNA).

Figure 5: System personal profile page (Olaniyi, Folorunso, Omotosho, & Alegbeleye, 2015)

The system covers eight unit of FUTMINNA healthcare centre and integrated as a system for two sites located at Gidan Kwano and Bosso campus linked together as a system for managing patient data, carrying out diagnosis and consultation regardless of location of the patient and healthcare practitioners. This was able to archived with aid of IoTs

4.3 Intelligent Community Security System

The intelligent community security system (ICSS) consists of four subsystems, which are; vehicle management subsystems, property management subsystem, theft and fire protection subsystem and environmental security subsystem. As shown in Figure 6, the information of each subsystem is sending to the community information processing Centre remotely for early alert and automatic adjustments in order to securing the community security.

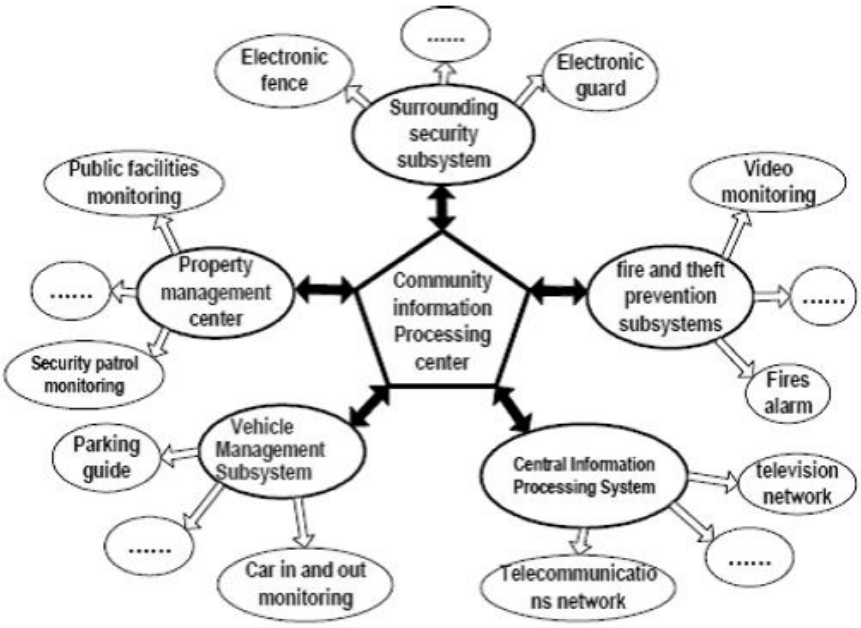

Figure 6: Intelligent Community Security System

5. SECURITY CHALLENGES IN IOTS

Security challenges in IoTs can be classified into technology challenges and privacy challenges.

5.1 Technology challenges in IoTs

IoTs is a virtually real world network system which interacts in a real time. Machine to machine (m2m) is the preliminary stage of IoTs (Bonomi, Milito, Zhu, & Addepalli, 2012), and it has unique development of context, support and features. Unattended function without intervention of human being is possible for a long time period through the WLAN/WAN. Though it delivering progressive in social efficiency, but it developed another set of new issue relating to security breach and privacy (Liu & Yang, 2011). Identified technology challenges in IoTs are follows;

5.1.1 Heterogenneity

Different entities with different vendors, capabilities and complexities are connected in IoTs (Brumitt, Meyers, Krumm, Kern, & Shafer, 2000). Some of these devices have dissimilar dates and different versions of release, it even using dismilar bitrates and technical interface, and altogether designed to perform different functions. However, if specific standards are not employ there may be conflict between IoTs machines.

5.1.2 Network

Network plays significant role in providing more widespread interconnectivity (Varshney & Vetter, 2002), thriftness of connetion and reliable quality of service. Owning to large number of devices sending data to enormous number of nodes, network congection may exist in IoTs machine which may resulted to denial of service (DoS) attack.

5.1.3 Front-end Sersor and Equipment

These are the equipment and sensor that collect data via the buil-in sensor and then transmit it using m2m devices modules. Owing to this function, achieving networking service of multiple sensor will occur. This approach comprises the security of machine and connectivity of nodes. Machine nodes are commonly distribued in the present of scenarios monitoring, and attacker can easily attack which imply unpermissive action on this node can be accomplished.

5.2 Privacy challenges in IoTs

Typically, in IoTs the environment is sense by the sensor attach to the machine and then transmits the gathering data and event to processing section that carries out the logic application. During the process of this activity, privacy of the users and protection of their data has been presented as the one of the significant challenges which required addressing in the IoTs (Cheng, Naslund, Selander, & Fogelström, 2012). Among the area in which privacy needs to be address are:

- Privacy issue in the devices
- Privacy issue during the communication
- Privacy issue in the storage
- Privacy during the processing of data

6. SECURITY COUNTERMEASURE IN IoTs

In order to provide countermeasure for the security threat, some of the countermeasure techniques required are follows:

6.1 Architecture Standards

Different devices, protocol and services are use by present IoTs to achieve unique objective. However, to improve a network of IoTs framework to attain a large structure, take for instant, to form a intelligent community system by incorporate various smart subsystems, there is need for a set of standards protocol that shoud be follow from the subsystem to the main system. This standard should comprise data model, interfaces and protocol that can support wide range of language, machine, operating system and humans.

6.2 Certification

The secure ways of confirming the true identity of the both parties that are communicate with each other is by certification. Hence, through the use of public key information (PKI), it is possible to attain the strong authentication by two ways public key certificate to ensure authenticity and confidentiality of the IoTs system.

6.3 Access Control

Another mechanism to ensure secure environment for IoTs system is by implemention of strong access control. The software oprrating on IoTs system shold ensure correct identification by certificate technique, and whenever an IoTs system is turning ON, it should authenticate itself first in the network before sending /collection of data. Since most of IoTs device have limited memory and computaion capability, therefore firewalling is requred in IoTs network to filter packet directed to the machines.

6.4 Data Encription

To prevent IoTs data form tampering and ensure confidentiality, data encryption is requred. When data is interfere by attacker, it prevents that data from being intercepted. Via the process of employ more secure key management and key exchange schemes, one can prevent attack on IoTs such as recording and replay, fabrication and eavesdropping (Weber, 2010).

7. FUTURE DIRECTIONS OF IOTs

IoTs has become a research area with a rapid growth in recent years in the area of Transportation, Telemedicine environment, Logistic and Pollution monitoring, etc. In a research carry out by (Leo, et al., 2014), they forecast that the number of things that will connected will raise up to 26 billion units by the year 2020. In another research of (Alsaadi & Tubaishat, 2015), they affirm the intention of UK governments to use smart energy monitoring system for all homes by year 2020. However, to enable sustainable of these IoTs devices and achieve its progress, challenges of IoTs must address. Following are the identified future directions for research to make IoTs more secure and acceptable;

a. Identity management.
b. Architecture standard.
c. 5G Protocol.
d. Session Layer

8. CONCLUSION

IoTs is an upcoming technology of innovation. With the IoTs technology short range mobile transceivers will be implemented in variety of daily needs, and the efficiency of information management and communications will ascend to a new high level. In order to make IoTs generally accepted, security and privacy are needed to be address by the researchers to build a trusted and secure environment for the delivery of IoTs.

REFEREINCES

1. Abomhara, M., & Køien, G. M. (2014). *Security and privacy in the Internet of Things: Current status and open issues.* Paper presented at the Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on.
2. Aghaei, S., Nematbakhsh, M. A., & Farsani, H. K. (2012). Evolution of the world wide web: From WEB 1.0 TO WEB 4.0. *International Journal of Web & Semantic Technology, 3*(1), 1.
3. Albert, R., Jeong, H., & Barabási, A.-L. (1999). Internet: Diameter of the world-wide web. *Nature, 401*(6749), 130-131.
4. Alsaadi, E., & Tubaishat, A. (2015). Internet of things: features, challenges, and vulnerabilities. *International Journal of Advanced Computer Science and Information Technology, 4*(1), 1-13.
5. Atzori, L., Iera, A., & Morabito, G. (2014). From" smart objects" to" social objects": The next evolutionary step of the internet of things. *IEEE Communications Magazine, 52*(1), 97-105.
6. Atzori, L., Iera, A., Morabito, G., & Nitti, M. (2012). The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization. *Computer Networks, 56*(16), 3594-3608.
7. Bing, K., Fu, L., Zhuo, Y., & Yanlei, L. (2011). *Design of an Internet of things-based smart home system.* Paper presented at the Intelligent Control and Information Processing (ICICIP), 2011 2nd International Conference on.
8. Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012). *Fog computing and its role in the internet of things.* Paper presented at the Proceedings of the first edition of the MCC workshop on Mobile cloud computing.
9. Borisov, N., Goldberg, I., & Wagner, D. (2001). *Intercepting mobile communications: the insecurity of 802.11.* Paper presented at the Proceedings of the 7th annual international conference on Mobile computing and networking.
10. Brumitt, B., Meyers, B., Krumm, J., Kern, A., & Shafer, S. (2000). *Easyliving: Technologies for intelligent environments.* Paper presented at the International Symposium on Handheld and Ubiquitous Computing.
11. Cheng, Y., Naslund, M., Selander, G., & Fogelström, E. (2012). *Privacy in machine-to-machine communications a state-of-the-art survey.* Paper presented at the Communication Systems (ICCS), 2012 IEEE International Conference on.
12. Crossman, D. M. (1997). The evolution of the World Wide Web as an emerging instructional technology tool. *Web-based instruction*, 19-23.
13. Fall, K. R., & Stevens, W. R. (2011). *TCP/IP illustrated, volume 1: The protocols*: addison-Wesley.
14. Friess, P. (2013). *Internet of things: converging technologies for smart environments and integrated ecosystems*: River Publishers.
15. Giusto, D., Iera, A., Morabito, G., & Atzori, L. (2010). *The internet of things: 20th Tyrrhenian workshop on digital communications*: Springer Science & Business Media.
16. Giusto, D., Lera, A., G., M., & Atzori, L. (2010). *The Internet of Things ISBN: 978-4419-1673-0*: Springer.
17. Karagiannis, T., Broido, A., & Faloutsos, M. (2004). *Transport layer identification of P2P traffic.* Paper presented at the Proceedings of the 4th ACM SIGCOMM conference on Internet measurement.
18. Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012). *Future internet: the internet of things architecture, possible applications and key challenges.* Paper presented at the Frontiers of Information Technology (FIT), 2012 10th International Conference on.
19. Kumar, J. S., & Patel, D. R. (2014). A survey on internet of things: Security and privacy issues. *International Journal of Computer Applications, 90*(11).
20. Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., . . . Wolff, S. (2009). A brief history of the Internet. *ACM SIGCOMM Computer Communication Review, 39*(5), 22-31.
21. Leo, M., Battisti, F., Carli, M., & Neri, A. (2014). *A federated architecture approach for Internet of Things security.* Paper presented at the Euro Med Telco Conference (EMTC), 2014.
22. Li, L., Xiaoguang, H., Ke, C., & Ketai, H. (2011). *The applications of wifi-based wireless sensor network in internet of things and smart grid.* Paper presented at the 2011 6th IEEE Conference on Industrial Electronics and Applications.

23. Liu, J., & Yang, L. (2011). *Application of Internet of Things in the community security management.* Paper presented at the Computational Intelligence, Communication Systems and Networks (CICSyN), 2011 Third International Conference on.
24. Olaniyi, O. M., Folorunso, T. A., Omotosho, A., & Alegbeleye, I. (2015). Securing Digitized Campus Clinical Healthcare Delivery System. *1st International Conference on Applied Information Technology*, 18-26.
25. Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2013). Context Aware Computing for The Internet of Things: A Survey. *IEEE Communications Survey & Tutorials*, 1-41.
26. Piscitello, D. M., & Chapin, A. L. (1993). *Open systems networking: TCP/IP and OSI*: Addison-Wesley Reading, MA.
27. Roman, R., Najera, P., & Lopez, J. (2011). Securing the internet of things. *Computer, IEEE, 44*(9), 51-58.
28. Sinph, J., Pasqueier, T., Bacon, J., Ko, H., & Eyers, D. (2015). Twenty Security Considerations for Cloud-Supported Internet of Things. *Internet of Things Jounal, IEEE*, 1-16.
29. Sproull, L., & Kiesler, S. (1991). Computers, networks and work. *Scientific American, 265*(3), 116-123.
30. Varshney, U., & Vetter, R. (2002). Mobile commerce: framework, applications and networking support. *Mobile networks and Applications, 7*(3), 185-198.
31. Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Bassi, A., . . . Eisenhauer, M. (2011). Internet of things strategic research roadmap. *O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, H. Sundmaeker, A. Bassi, et al., Internet of Things: Global Technological and Societal Trends, 1*, 9-52.
32. Weber, R. H. (2010). Internet of Things–New security and privacy challenges. *Computer Law & Security Review, 26*(1), 23-30.
33. Werle, R. (2001). Internet@ Europe: Overcoming institutional fragmentation and policy failure. *European Integration online Papers (EIoP), 5*(7).
34. Zhao, K., & Ge, L. (2013). *A survey on the internet of things security.* Paper presented at the Computational Intelligence and Security (CIS), 2013 9th International Conference on.