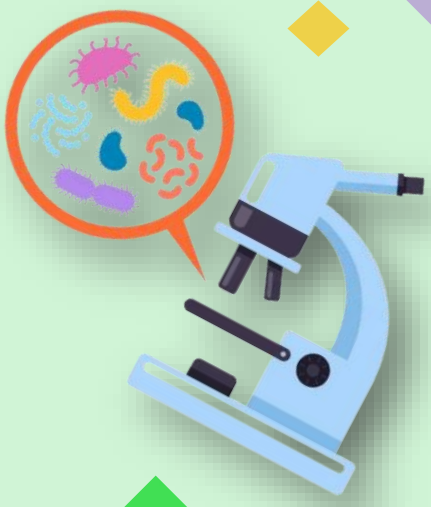
I CONGRESO INTERNACIONAL
DE CIENCIAS EXACTAS Y NATURALES
COSTA RICA, DEL 4 AL 7 DE JUNIO DE 2019

# I Congreso Internacional de Ciencias Exactas y Naturales

**Editado por**
**Yuri Morales López**



**Universidad Nacional**
**Costa Rica, 2019.**

**ISBN: 978-9968-9661-6-0.**

FCEN
Facultad
Ciencias Exactas y Naturales

I Congreso Internacional de Ciencias Exactas y Naturales/ Yuri Morales-López –Heredia, Costa Rica: Universidad Nacional, 2019.

ISBN: 978-9968-9661-6-0.



**Reconocimiento**

Se les agradece profundamente a la Bachiller Evelyn Rojas Ramírez y al Máster Luis Ocampo Venegas por el apoyo para la gestión de este documento.

# Basic Security System requirements for IoT-based Smart City Network-layer

**Majid Bayani-Abbasy**
mbayani@una.cr
Universidad Nacional
Costa Rica
**Oscar Ramírez**
Oscramir@cisco.com
Cisco Systems
Costa Rica

**Resumen:** Uno de los tópicos emergente de socio técnico basado en tecnología de Internet de las cosas (IoT) se llama ciudades inteligentes. Una cuidad inteligente es una colección de objetos y entidades en una área socio técnico urbana que sus componentes siempre están en línea conectado y auto servido. En este articulo se considera que una ciudad inteligente consiste en varios módulos que se necesita constantemente monitoreados para detectar las brechas de seguridad para bajar los factores de riesgo a las personas. Este trabajo provee una explicación breve acerca de los problemas de seguridad en diferentes capas de una estructura de IoT. Un marco teórico basado en componentes de la capa de redes en ciudades inteligentes esta desarrollado en este trabajo. Al final, depende de diferentes ataques internos e externos una lista de requerimientos de sistema se presenta en detalles.

*Palabras clave*: Ciudades inteligentes; Seguridad; Internet de las Cosas; ataques;

**Abstract**: Smart city is an emergent topic of social and technical concept based on the IoT technology. A smart city is defined as a collection of objects and entities in a socio-technical urban area that their components are always connected online and self-automated. In the context of this research a smart city consists of several full-aware modules that need to be monitored constantly to detect security holes in order to diminish the risk factors for people. This paper firstly, provides a concise explanation of the security issues in different layers of an IoT-based structure. After that, a basic component-based framework of smart city network-layer presented. Finally, depends on type of external or internal attacking, a list of system requirements were discussed in details.

*Keywords*: Internet of thing (IoT); Security; Smart City; Network Layer.

## Introduction

The main idea of connecting the all objects is routed from a historical path while in the 1970s, for the first time, the microprocessors were created and come into the human business world. That was followed in the 1980s by enabling the first Internet appliance connection (Carnegie Mellon University, 2015). Mark Weiser presented the ubiquitous computing in 1988 (Friedemann and Floerkemeier, 2010 ;Weiser,1991). For the first time the first toaster appliance was connected to a computer through TCP/IP in the last decade of the 1980s (Buddy, 2017).

At the same decade, the idea of Distributed Sensor Network was originated by DARPA

Tema: Gestión del riesgo y reducción de la vulnerabilidad.
Principal área: Informática

Bayani-Abbasy, M. & Ramírez, O. (2019). Basic Security System requirements for IoT-based Smart City Network-layer. En Y. Morales-López (Ed.), *Memorias del I Congreso Internacional de Ciencias Exactas y Naturales de la Universidad Nacional, Costa Rica, 2019* (e221, pp. 1-12). Heredia: Universidad Nacional. doi http://dx.doi.org/10.15359/cicen.1.75

project. Finally, A decade later, in 1999, Kevin Ashton, a British entrepreneur, invented the term of Internet of Things [IoT] for the first time while was working at Labs Auto-D centers, referring to the RFID) (Silicon Labs, 2013). The basic idea of the a concept and model based on the connection of objects like Radio Frequency Identification tags was introduced by Kevin Ashton, while was working at Labs Auto-ID centers a decade later in 1999 (Wood,2015; Parashar, Khan and Neha,2016). Internet of things (IoT) is based on the internetworking of the physical objects in order to collect/exchange the sensory data using the unique IPv6 addressing schemes. The Global Standards Initiative on Internet of Things (IoT-GSI) defined IoT as the global infrastructure for the information society in order to provide the massive interconnecting of the physical objects (IoT-GSI, 2012). And also, the Internet society (ISOC), defines the IoT as the network infrastructure connectivity includes the physical objects & device in order to perceive the sensory information without human interference (ISOC. 2014). IoT also, facilitates the machine-to-machine connectivity of devices as well as systems through the cloud technology (Höller et al., 2014) and until now, a few IoT applications were developed. It is predictable in the close future, there will be developed a large number of the applications for smart IoT systems [11]. The scope of its application and the technologies such as WSN and RFID that support it is expanded form the smart to the complex IoT ecologies. In fact, IoT applications embrace all human activities. IoT comprises all macro human/object activities. As it develops, it expands in size, and scale of influences the context of our life involving more and more devices (Bayani, and Vilchez,2017) .On the other side with increasing the high implementation rate of IoT, more everyday objects connected to the global IoT Internet network and logically is converting to the accessible target for data security risks; In this way, IoT in the magnitude of its volume, has a big potential to distribute, and attract these risks faraway than the Internet has, up to now. Some of these risks are due to the risks that are coherent and comes with the same objects and some of others are structural that has been converted to a big challenge and concern (Kumar,Vealey, and Srivastava, 2016 ;Kumar, Vealey and Srivastava,2016). Firstly, this paper presents a concise analysis of the general layer-based IoT security consideration. After then, several security concerns related to the network security of smart cities will be discussed in the second part as long as a conclusion and recommendation to the threads. A state of art related to the investigated topic will be discussed in the following.

## RELATED WORK

Engin Leloglu (Leloglu,2017), has been explained a review of security concerns in IoT. He defines the security requirements and challenges that are common in IoT developments. He discussed in his study the security threats and their solutions on each IoT layer to make a secure technology. Based on Muhammad A. Iqbal et al. (Iqbal, Oladiran,Magdy, and Bayoumi,2017), conventional security policies due to the different communication protocols and stacks in IoT cannot be applied actually to the IoT system architectures. This is because of the heterogeneous IoT structure, devices, lack of resources. He suggests a strong network security infrastructure in order to protect data security risks. Some main IoT constraints and security challenges and concern are addressed in (Shipley, 2015). In (Kumar,Vealey, and Srivastava, 2016 ;Kumar,Vealey and Srivastava,2016) Sathish A. Kumar et al. present a review of security IoT-layer based attacks in some example scenarios as along as a methodology solution for those issues. They also, draw a concise list

of existing security methods and limitations the reliability for IoT and proposing a security framework to overcome these limitations. Security against efficiency as an actual problem for IoT products is detailed in (Kostadinov, 2015), by Dimitar Kostadinov. He concluded that is not clear at the present time what option should be considered as the proper answer to applying the integrity, availability and confidentiality availability procedures without influencing undesirably the distributed computational resources and energy optimization. Chris et al. in (Folk et al., 2015) proposed a method in order to better define the threat opening that can change with the new socio-technical environment created by IoT. Their recommendation is "IoT development must include security without effort as virtually no consumer is an IT security expert. This must include the interplay between device ecosystems—users cannot be expected to perform positive actions to make up for security flaws." Security threats and vulnerabilities concern related to the smart cities was analyzed by Sidra Ijaz et al. in (Ijaz et l., 2016). They proposed some best practices based on the three factors: technological, socio-economical and governance factors. Cyber-security challenges such as privacy, safety and security in smart cities also discussed by Adel S. Elmaghraby and M. Losavio in (Elmaghrabyand Losavio, 2014). M. Georgescu and D. Popescul in (Georgescu,and Popescul,2016), have presented an extensive overview of security-related issues in the smart-cities framework. The paper talked about security vulnerabilities and threats in internet of things with the intention of raising public interest awareness. The issues such as heterogeneity, ubiquity in context of the IoT Security were discussed by authors. They think the urban managers should manage wisely the concepts of risk and security as well as the privacy. And also the authorities should be well-informed about all issues related to smart city security. This paper is a concise explanation related to the security concept in the general IoT architecture and tries to give a different vision about the IoT smart cities security problems.

**Internet of Thing System Architecture**

Basically, the most common architecture of IoT consists of the three layers (Sethi and Sarangi, 2017), that is shown in Figure 1:

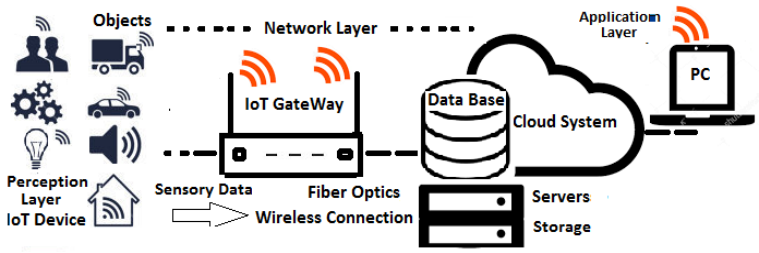



Figure 1. The basic 3-layer Architecture of IoT

The physical layer is the perception layer that includes the sensing devices. This layer is in charge of collect the sensory data and sends them to the gateway and then delivers them to the cloud system in order to further process. The Network layer provides connection between the smart devices gateway cloud and servers as well control signaling. And finally, the application layer the user interface interacting with the other layer and providing the various services for users.

### *Technologies that support IoT*

IoT employs a set of technologies such as Internet, RFID and Wireless Sensor Networks (WSNs) in order to provide connectivity between nodes (Pujara and Satyanarayanab, 2015). WSNs includes sensor nodes to sense the events and activities and send the data to the base station point (sink) to further process . The Radio Frequency Identification Device (RFID) is another technology which RFID provides unique identification of the objects and enables to track them. Figures 2 and 3 demonstrate the basic structure of the RFID and WSN technologies.


Figure 2. A Simple structure of the RFID platform

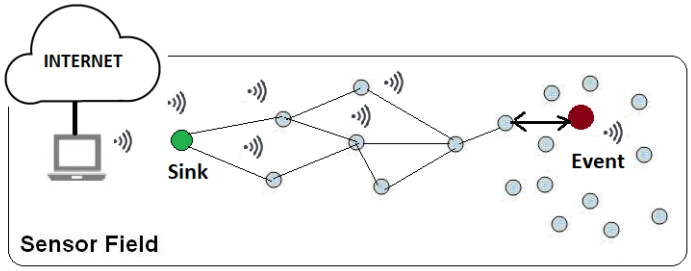



Figure 3. Basic WSN architecture (Bayani et al., 2018)

### *Security concerns*

Based on the basic IoT model, the security concerns in each layer will be discussed in the following.

A. Perception layer Security issues

All traditional Internet security concerns in addition to the IoT adopted security issues are the security matters. The threats in this layer are related to the sensing node, radio signals and physical attacks (Xiaohui, 2013; Pawar and Chillarge,2017; Vijayalakshmi and Arockiam,2016). Node and Device Security: RFID, RSN, NFC and wireless sensor mote devices are two main technologies that support and drive IoT. All vulnerabilities associated to these technologies, automatically converts to the IoT device weakness. The security risks, such as the sniffing the node, spoofing, link layer attack, data loss , tag tracking, power control ,flooding attack , hardware node failure & damage, node attacking, false or noise contaminated sensory signal.

B. Network Layer Security issues

The fist concern in this layer is the “connectivity”. This layer can act as the intermediate layer between user application and the perception layer. It is highly vulnerable to attacks due to the high volume of the information that should be carried to the cloud

system. A bottleneck or network congestion, DOS, storage, un-authorized attacks can be as a serious thread (Kumar,Vealey, and Srivastava,2016),. The main security issues can include the WiFi, Bluetooth, and Infrared, 3 & 4G access network, transmission line security, signalling, LAN, WAN & protocol security ,as well (Vijayalakshmi and Arockiam, 2016).

C. Application Layer Security issues

What can be happened in this layer are in the software levels. After a successful attack in this layer, application can be bargained or shut down. A denial of service is a typical consequence security issue. Malicious code attacks, data leakage, data overloading, data loss, data authentication, interface & software corruption, mobile computing threads, OS failure, conventional windows/OS mobile-based viruses, are listed as the main issue in the IoT application layer.(Kumar et al.,2016; Suo et al., 2012; Xiaohui, 2013; Pawar and Chillarge,2017; Kozlov,Veijalainen, and Ali,2012).

**Smart Cities: Network Layer Security Issues**

The smart cities are considered as a socio-technical system. Smart city is a socio-technical collaborative information system, that technologies such as Internet, ICT, cloud computing, virtualization and IoT support its development. Actually, smart cities employ IoT in order to implement their components and improve their service efficiency and also encourage their citizen to involve all social-technical activities. As IoT develops, more connected objects are pervasive and used in smart city deployments. Thus, more security issues and more potential cyber threats will emerge to cope with them (Georgescu and Popescul, 2016; Dustdar, Nastić,and Šćekić,2017); Bawany, and Shamsi, 2015; Talari et al. 2017).

There are a list of striking attacks that can be done by intruders in the network layer such as: Sleep deprivation, Homing, MITM attack, DoS ,Misdirection ,Acknowledgment spoofing Integrity, malicious code ,Spoofed, altering routing information Integrity, transmission threads, Wormhole, routing attacks , protocol issues, Networking connectivity ,Sybil Integrity, Hello flood, physical disruptions, Sinkhole and Internet Smurf Integrity (Garcia-Font et.al,2017; Li, and Xu,2017; Bartoli et al., 2011; Elmaghraby,2013).

Although the security issues of the smart cities are layered-based, but the most challengeable dangerous attacks could be attempting to shut down the global communication network. IoT structure is based on the wireless technology connections which require high-speed broadband communication with a great rate of transmission. The connection is based on a combination of the fiber optics, 3G/4G, Bluetooth, ZigBee, LTE technologies to bring connectivity to a numerous of services. Communications system that is typically a combination of wired and wireless networks (Nissan, 2017),. A shut down attack on the communicating system can make entire disrupt overall system. This can be conducted by several malicious intruders vs. wireless telecommunication infrastructure. Such attacks have a big potential to disrupt communication network, consequently impacting its overall networks and service (Sechel, 2016; Georgescu and Popescul, 2016).The intruders can either be come from internal or external zones.

A. External attacks

Possible external intrusion from outside of the structure: Attackers should pass several layers in order to reach to the service layer.

B. Internal attacks

The malicious user (local hackers) intents to shut down any service attempting to realize a DoS attack from inside of the network.

Figure 4, demonstrates a smart city scheme includes network layer and service sub-layer and most important components that can be a target for hackers.

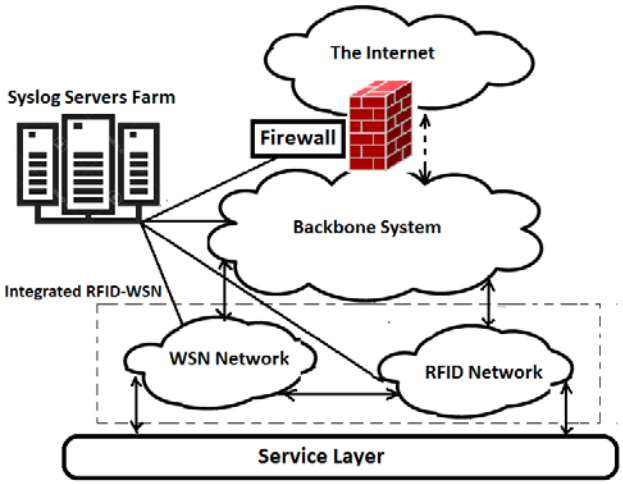



Figure 4. a smart city basic security structure

If an invader going to reach to the sub-service layer from outside, should cross at least three tiers such as a robust firewall, Backbone, an Integrated WSN-RFID network, gateway and finally the service layer and application. In this direction, a proper configuration in different phases can be an obstacle vs. the intruder while a sys-log server center monitors all authorized and unauthorized tracks and movements.

The security requirements in this layer should involve: (Suo et. al., 2012; Dustdar, Nastić and Šćekić, 2017; Kreutz et al., 2015; Nissan, 2017 and Leo et al.,2014). They are listed in the following:

1) An overall system protection

This includes security requirements for each level such as: availability, key protection, integrity confidentiality, identity, Authentication process, Trust Establishment.

2) Firewall configuration

A set of applications controls the functions (management plane). It is desired to implement network control in order to filter the authorized and unauthorized traffics. This includes applications such as firewalls and/or load balancers. The main policies, instructions and access-lists will be configured in the firewalls by a MP.

3) Communication monitoring

Communication within smart cities comprises multiple combinations and access networks with cloud-computing platforms. A constant communication real-time traffic and managing monitoring, needs to check the functionalities. The sys-log servers can store all tracks related to the linking state between backbone and integrated RFID–WSN system, bandwidth, speed and broadcast checking (fake storm flooding), confidentiality & integrity of signaling, over connected ,as well as connection between gateway and upper/lower layers.

4) Hardware failure monitoring

Include a continuous and periodic maintenance of the equipment such as: Firewalls, cable connections, routers and backbone switches.

5) Gateway compromising

In smart cities as Figure 1 depicts, the network gateways are the intermediary between the perception layer and the cloud-system by receiving, aggregating, small processing, filtering and transmitting sensory data to the cloud-system platform. IoT devices perform an authentication process to the local gateway when sending the captured data and gateway should realize the authentication process to the cloud system, as well. Collision, jamming, and gateway compromising are results of the existing a black hole at a gateway. A complete analysis on the gateways with conventional real-time security tools is required.

***Importance of the Socio technical security in the smart cities***

Electronic interaction between people, IoT technology and platform in the smart city can generate serious security concerns. Protecting IoT architecture against vulnerabilities can accomplished in different level of the communication. As said before, user authentication is the first and basic step of the shield in an intelligent community (service layer). They are considered as the basic element or agent. Safety of the communication lines between the basic agents with the second layer (WSN and RFID networks) guaranty connection between all objects in the smart city. What was discussed in the previous section is related to the warranty of network layer. In other words, RFID and WSN protection will be the principal strategy in this line (Laeeq and Shamsi, 2015). The operational security requirements of a smart city are to guarantee that the IoT technology and infrastructure are safe against any cyber-attack different level. Also, another big concern is associated to the data generation and communication between various elements in the platform. However, the data generation safety and system shielding is reliant on the whole network layer security in such a way, an intruder can break into the system, violating the data access policy in case of existing any unsecure hole or vulnerabilities (Butt, and Afzaal, 2019).

## CONCLUSION

Overall research challenges can be classified into the following aspects: security in the IoT system architecture layers and specifically in the network layer of the smart cities. Network-layer security issue in the socio-technical environment of the smart cities is a main concern for those researchers that are trying to decrease and mitigate impact of the predictable damages or disrupts coming from a misconfiguration or ignoring the security measures. A structural view of the network layer for a smart city is presented in this short research in order to discuss the possible solutions or strategy to cope with the disregarding of a local or external attack. As resources of either internal or external entities are different, the protection strategies or policies that are employed are not the same. An alert awareness monitoring system is required in the right place of the whole topology along with a sys-log server centers in order to track all strangers' activities, , architecturally. These servers are connected to the backbone and an integrated RFID-WSN system in order to locate as close as possible to the events. Finally, it is suggested to implement the necessary hardware and software installation and performing a list of real-time activities proposed to manage the security risk issues in the different part of the network layer in a typical basic smart city scenario.

## Reference

Carnegie Mellon University. (2015), The Only Coke Machine on the Internet", Computer Science Department, n.d. Web. 06 Sept. 2015. URL: http://www.cs.cmu.edu/~coke/history_long.txt.

Friedemann,M. and Floerkemeier,C.(2010). "From the Internet of Computers to the Internet of Things". Informatik- Spektrum. Vol. 33, Issue 2, April 2010, pp 107–121.

Weiser,M. (1991) "The Computer for the 21st Century," Scientific American. Bibcode: 1991SciAm.265c.94W, Vol. 265, Issue 3, 1991, pp 94–104.

Buddy,M. (2017) "Brief history of the internet of things," Jun 15, 2017, URL: http://mqtt.ximxim.com/brief-history-internet-things/.

Silicon Labs. (2013). "The evolution of wireless sensor networks," .URL: http://www.silabs.com/Support%20Documents/TechnicalDocs/evolution-of-wireless-sensor-networks.pdf., 2013.

Wood,A. (2015), "The internet of things is revolutionizing our lives, but standards are a must," Theguardian.com. Guardian. Retrieved 31 March 2015.

Parashar,R., Khan,A. and Neha. (2016), "A Survey: The Internet of Things", International Journal of Technical Research and Applications, e-ISSN: 2320-8163, Vol. 4, Issue 3, (May-June, 2016), pp. 251-257.

IoT-GSI. (2012), "Internet of Things Global Standards Initiative", February 2012, URL:

http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx

ISOC.(2014), “The Internet of Things (IoT): An Overview “Understanding the Issues and Challenges of a More Connected World, Oct 2015, URL: https://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151014_0.pdf.

Höller,J.,Tsiatsis,V., Mulligan,c., C. Karnouskos, S. ,Avesand,S., and Boyle,D..(2014), “From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence,” Elsevier, 2014, ISBN 978-0-12-407684-6.

Bayani,M. and Vilchez,E. (2017), “"Predictable Influence of IoT (Internet of Things) in the Higher Education," International Journal of Information and Education Technology ,vol. 7, no. 12, pp. 914-920, 2017.

Kumar,S.A.Vealey,T. and Srivastava,H..(2016), “Security in Internet of Things: Challenges, Solutions and Future Directions,” Proceedings of the49th Hawaii International Conference on System Sciences (HICSS), p.5772-5781, January 05-08, 2016. [Doi>10.1109/HICSS.2016.714].

Suo,H.,Wan,J., Zou,C., JLiu,J.(2012), “Security in the Internet of Things – A Review,”International Conference on Computer Science and Electronics Engineering (ICCSEE) , pp 648 –651.

Leloglu,E..(2017), “A Review of Security Concerns in Internet of Things”, Journal of Computer and Communications, 2017, Journal of Computer and Communications, vol. 5, pp. 121-136, doi: 10.4236/jcc.2017.51010.

Iqbal,M.A., Oladiran,G. , Magdy,A. and Bayoumi,A. (2017), “A Review on Internet of Things (IoT): Security and Privacy Requirements and the Solution Approaches,” Global Journal of Computer Science and Technology, [S.l.], Jan. 2017, ISSN 0975-4172.

Shipley,A.(2015), “Security in the Internet of Things-Lessons from the Past for the Connected Future,” White paper, 2015, Wind River Systems, Inc. http://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf.

Kostadinov,D. (2015), “Security Challenges in the Internet of Things (IoT)”, URL:http://resources.infosecinstitute.com/security-challenges-in-the-internet-of-things-iot/#gref, Posted in Security Awareness on November 30, 2015.

Folk,C., Hurley, D.C., Kaplow, W.K. and Payne, J.F.X.(2015), "The Security implications of the Internet of things," The AFCEA International Cyber Committee White Paper Series, Feb. 2015, https://www.afcea.org/site/sites/default/files/files/AFC_WhitePaper_Revised_Out.pdf.

Ijaz,S., Shah,M.A., Khan,A., and Ahmed,M. (2016) "Smart Cities: A Survey on Security Concerns", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No.2, 2016.

Elmaghraby,A.S. and Losavio,M.(2014), "Cyber security challenges in Smart Cities: Safety, security and privacy", Journal of Advanced Research Volume 5, Issue 4, July 2014, Pages 491-497.

Georgescu,M. and Popescul,D. (2016), "The Importance of Internet of Things Security for Smart Cities", Book chapter, Smart Cities Technologies Edited by Ivan Nunes Da Silva and Rogerio Andrade Flauzino, ISBN 978-953-51-2808-3, Print ISBN 978-953-51-2807-6, 244 pages, Publisher: InTech, Chapters published December 07, 2016 under CC BY 3.0 license, DOI: 10.5772/61375.

Sethi,P. and Sarangi,S.R. (2017), "Internet of Things: Architectures, Protocols, and Applications." Journal of Electrical and Computer Engineering, Vol. 2017 (2017), Article ID 9324035, 25 pages.

Xiaohui,Xu. (2013), "Study on Security Problems and Key Technologies of The Internet of Things," Fifth International Conference on Computational and Information Sciences (ICCIS), pp.407–410, 2013.

Pawar,M. and Chillarge,G.(2017), "Security and Privacy in IoT", International Journal of Modern Trends in Engineering and Science, Vol. 04, Issue 05 2017, ISSN no: 2348-3121, Page no: 18-23.

Vijayalakshmi, A. V. and Arockiam,L. (2016), "A Study on Security issues and challenges in IoT", International Journal OF Engineering Sciences & Management Research, IJESMR, IJESMR, 3(11), Nov.2016, ISSN 2349-6193, pp.34-43.

Kozlov,D., Veijalainen,J. and Ali,Y. (2012), "Security and Privacy Threats in IoT Architectures," in Proceedings of the 7th International Conference on Body Area Networks, ser. BodyNets '12. ICST2012, pp. 256–262.

Dustdar, S., Nastić,S. and Šćekić,O.(2017), "Smart Cities: The Internet of Things, People, and Systems," book 2017: ISBN: 978-3-319-60029-1 (Print) 978-3-319-60030-7

(Online), DOI: 10.1007/978-3-319-60030-7. Publisher: Springer International Publishing.

Bawany, N. Z. , and Shamsi, J. A. (2015) , "Smart City Architecture: Vision and Challenges," (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 6, No. 11, 2015.

Talari,S., Shafie-khah,M., Siano,P., Loia,V., Tommasetti,A. and Catalão, J.P.S.(2017), "Review of Smart Cities Based on the Internet of Things Concept," Energies 2017, 10(4), 421; doi: 10.3390/en10040421.

Garcia-Font,V., Garrigues, C. and Rifà-Pous,H.(2017), "Attack Classification Schema for Smart City WSNs", Sensors 2017, vol. 17, No. 771; doi.10.3390/s17040771, www.mdpi.com/journal/sensors.

Li,S. and Xu, L.D.(2017), "Securing the Internet of Things", book, ISBN-13: 978-0128044582, ISBN-10: 0128044586. Publisher: Syngress; 1 edition, Jan. 30, 2017,154 pages.

Bartoli,A.,Hernandez-Serrano,J.,Soriano, Dohler,M.,Kountouris,A. and Barthel,D.(2011), "Security and Privacy in your Smart City," proceedings of the Barcelona smart cities congress, 2011, Spain.

Elmaghraby,A.S.(2013), "Security and Privacy in the Smart city," proceeding of 6th Ajman International Urban Planning Conference AIUPC 6: City and Security, 11-14 Mar. 2013.

Sechel,S.(2016), "Information insecurity: an assessment of the Romanian cyberspace," In proceedings of the 15th International Conference on Informatics in Economy (IE 2016), http://dx.doi.org/10.5772/65206, 2016, pp.314-320.

Kreutz,D., Ramos, FMV., Verissimo,PE, Rothenberg,CE.,Azodolmolky,S. and Uhlig, S.(2015), "Software-Defined Networking: A Comprehensive Survey", Proceedings of the IEEE | Vol. 103, No. 1, January 2015. https://arxiv.org/pdf/1406.0440.pdf.

Nissan,Y.(2017), "Addressing smart city communications." CCTV, Surveillance & Remote Monitoring, IT infrastructure, Apr. 2017, URL: http://www.securitysa.com/7908r.

Leo,M., Battisti,F., Carli,M., and Neri,A.(2014), "A federated architecture approach for Internet of Things security," in Euro Med Telco Conference (EMTC), 1-5, 2014.

Bayani, M., Segura, A., Alvarado, M., & Loaiza, M. (2018). IoT-Based Library Automation and Monitoring system: Developing an Implementation framework of Implementation. *e-Ciencias de la Información*, Vol. 8 No. 1, pp. 3-18.

Laeeq,K., Shamsi,J,A. (2015), A study of security issues vulnerabilities and challenges in internet of things", Securing Cyber-Physical Systems, pp. 221, 2015.

Butt, T.A., Afzaal, M. (2019), Security and Privacy in Smart Cities: Issues and Current Solutions. In: Al-Masri A., Curran K. (eds) Smart Technologies and Innovation for a Sustainable Future. Advances in Science, Technology & Innovation (IEREK Interdisciplinary Series for Sustainable Development), Springer, Cham