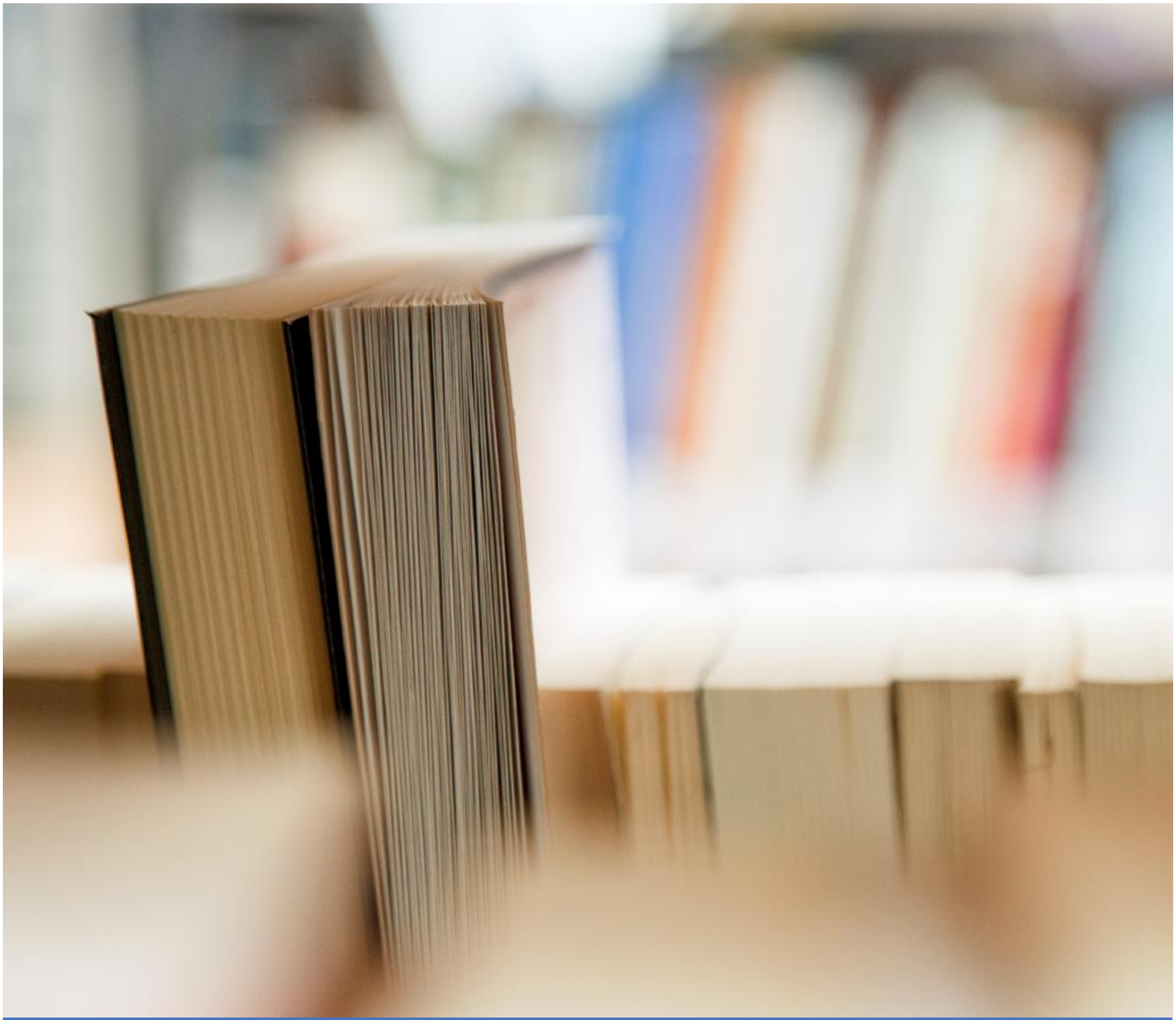

Smart City - Internet of Things (IoT) Security

Quoc Lap Trieu - 19263045

Quoc Lap Trieu 10/29/18 Systems and Network Security

Contents

I. Introduction

Internet of Things (IoT) has been one of the main interesting areas in recent years. By equipping small sensor devices with the ability to transfer data, these devices are able to communicate with each other, creating a part of an Internet network [1]. Due to the development of IoT and the necessity for improving services for the citizens in a city, a new concept has been realized, the Smart City. With the purpose of providing the supports for different services in the city, Smart City aims to develop a system that could integrate small devices with a back-end server system for processing data and a user interface application for accessing information.

The rest of this essay is organized as follows. The second section focuses on the main part of the topic. More in detail, this section contains the three subsections that fully discuss the application of the Internet of Things (IoT), its security issues and how to address those issues in order to improve the reliability of the application. The final section is the conclusion of this essay, in which the author would like to summarize the whole idea and give his points of view about this topic.

II. Smart City – An IoT Application

1. Application:

In this section, the author would like to describe more about the application in the area of IoT, which is the Internet of Thing project for smart cities. This application has been a popular topic for researchers as there are many publications relating to this topic proposing new approaches as well as solutions to develop a smart city [2]. It is defined as a way of supporting the idea of Smart City vision, which focuses on using advanced technology devices to communicate with each other and provide a better service for citizens as well as the cities. In other words, Smart City aims to utilize the public resources to improve the quality of services for citizens such as improving a better system alarm for traffic congestion but reducing the costs of operating the system. By collecting GPS information from cars or motorbikes, the system is able to monitor the current traffic congestion information of a particular location. Because of that, end users could be able to adjust their directions to avoid the traffic.
Error! Reference source not found. indicates 9 types of service that Smart City provides in order to enhance the quality of life for the citizens and the development of the city.

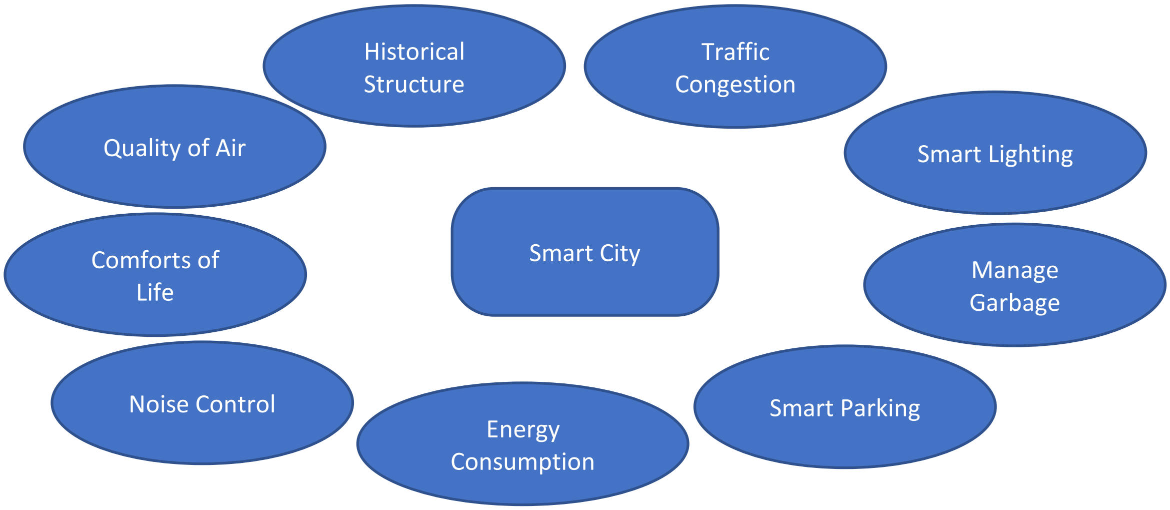

Figure 1. Services of Smart City

The Smart City application is a combination of a group of peripheral devices distributed around the city and a centralized center. The peripheral devices or device nodes are usually small sensors with the purpose of collecting different kinds of data in vicinity environment and delivering it to the centralized center or the control system using data link layer network communication [3]. The controller system is responsible for handling complex tasks such as processing and analyzing the collected data in order to make decisions.

On the one hand, due to the fact that the sensor nodes are usually small devices with low power and limited processing capability, they are equipped with the different types of link layer technologies such as Bluetooth or NFC. On the other hand, because of the necessity in high-speed transmission rate for large data, the technologies for the link layer of the centralized center are usually the traditional communications with high reliability such as Wireless network connection or fiber optic.
Because of that, it goes without saying that between these device nodes and the center system, there needs to exist a communicator for the purpose of converting and transferring the data between them [3]. This communicator is usually called as a gateway, which is distributed at the locations near device nodes as indicated in **Figure 2**, which is the simple structure of the Smart City system.

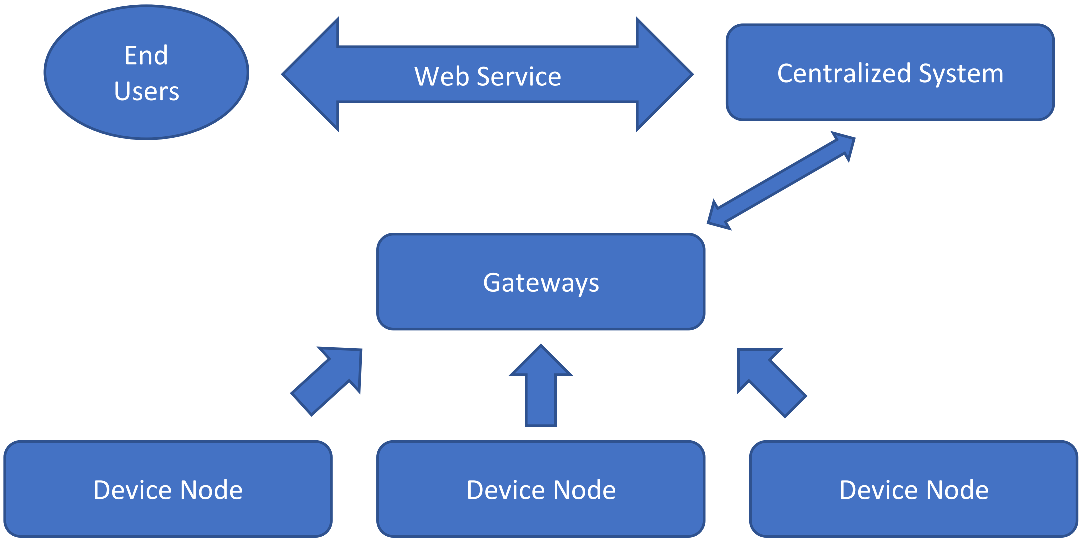

Figure 2. A Simple Structure of Smart City

2. Security Issues

The problem of Security is one of the main major points in any network application. The Smart City project also brings out many challenges in the security area. There have been many reports relating to security attacks of Smart City and a large amount of data are also compromised by attackers [4]. Regarding the issues in the security of a network application in general or the Smart City project in particular, there are four are areas of security that should be concerned [5]:

First, it is the confidentiality of the information to be transferred over the Internet. The data that contains sensitive information could be read by the third party during the transmission process between the client and server or device nodes and gateways. As the development of sensor devices, data collected from sensor devices is sometimes sensitive and could affect users' privacy. For example, attackers could be able to access the GPS information a family to detect whether they are at home or not. This could be dangerous in case of burglary.

The second area of security needs to be mentioned is the authenticity of the information. An attacker could falsify the sender identification and send the data to the receiver with malicious intent. For example, an attacker uses his device to stimulate a temperature sensor to send the wrong information about the current temperature in a particular location to the server [4]. Because of this, the centralized system could process, analyze and send to end users the incorrect information.

The integrity of the information is considered as the third major concern for an IoT application. In this area, the data between the sender and receiver could be modified by the third party for different purposes. Instead of falsifying the identification of the sensor nodes, attackers could also try to capture and modify the content of the packets by using the Man-in-the-Middle (MITM) attack.

The final concern is about the availability of the information. A system needs to guarantee the information is always available for users to access. A common cause of unavailability of data is Denial of Service attack (DoS), in which the attackers sending a large number of requests to the server in order to overwhelm the processing capability of the system. For example, if a user wants to access the web application to check the traffic information at his current location in order to adjust his direction properly to avoid traffic congestion. However, due to some issues in the security system, the server is not available to gain access to the traffic data, affecting the reliability of the Smart City system.

Besides, [3] mentions that sensor nodes are usually low-power devices and are equipped with low-reliability communication technologies such as Bluetooth and RFID. It is also true that these types of link layer technologies are usually not constructed with strong security protection because of its simple structure. Because of that, it is convenient for attackers to gain access to the information during the transmission between devices nodes and data controller.

Attackers could also use malware to gain access to the system. The paper [5] mentions Linux.Darlloz Worm as a type of malware which is used to attack home routers or gateways and based on that it could help attacker access to the main central system. It is also worth to consider that according to [6], Stuxnet has been published on the back market since the year of 2013. It is the malicious piece of code that could be used to target a different type of devices and exploit various types of the vulnerability of the system.

3. Security Solutions:

In order to address the issues in a security mentioned in section 2, researchers have been proposed different methods to deal with different types of attack. In regard to the confidentiality of the information, it is best to encrypt data at the sensor nodes before sending them out. In the connection between end users and the web application, it is suggested that the connection should be encrypted by using virtual private connection (VPN) that creates a connecting tunnel between the two parties and only them can access to the information in that tunnel [7]. In this case, a VPN server needs to be available for establishing the connection, the problem of whether it is a rented or hosted VPN server depends on the organization.

In case of authenticity issue, certificates are used as an identification in the network communication. By using public key infrastructure, certificates are applied on gateways to authenticate in sending to and receiving data from the central server. Also, [8] mentions that trusted platform module (TPM) could be used on gateways as a function to provide the service of identifying devices in order to make sure that the received data from a sensor node is actually delivered from that node. The problem of integrity could be addressed by using the common method of combining digest and encrypted data. The server could be able to verify the information based on the digest which is generated by hashing algorithms. The availability of information could be ensured by providing a powerful centralized machine. Also, it is necessary to apply techniques such as blocking IP or firewall protection at the central system.

Besides these four major areas of security, it is also essential to consider that every new device before accepted to the Smart City network must be done via the process of testing. It is suggested that integration testing and functionality testing should be done first in order to detect vulnerabilities since this could affect the whole existing network significantly [5]. Beside the technical solutions in addressing the security challenges of Smart City, it is also important to note that the public's awareness about security issues of the IoT network is also essential. Citizens and hardware providers are required to understand the importance of the legal framework and how to develop programs that follow security standards in order to avoid the vulnerabilities of the system.

The paper [2] suggests that instead of building a vertical IoT model, it is best to consider the idea of having one horizontal IoT platform in order to reduce the attacks from hackers. A vertical model depends completely on one organization, which is good in the issue of compatibility between devices, but lacking innovation as well as support. However, a horizontal IoT model utilizes multiple providers on one common framework to operate. This model allows the community of developers to join, develop, and improving the solution effectively, which minimizes the attackers from the third party.

III. Conclusion

In this essay, the author focuses on the description of the Smart City project including the overview of the application, the main issues in the security area, and solutions of the project. In the problems of security, the author indicates the four major areas that every network application needs to deal with, which are confidentiality, integrity, authenticity, and availability. Besides, the author also suggests solutions that could be applied in order to avoid main attacks from outside. Even though plenty of approaches to improve the performance as well as to handle security issues in Smart City have been proposed by researchers, there still exists security challenges that require a better solution for the future of IoT. For this reason, the idea of a perfect Smart City that utilizes advanced technologies to support better services for citizens with high reliability is still a long way to go.

IV. References

[1] A. I. a. G. M. L. Atzori, "The internet of things: A survey," *Comput. Netw,* vol. 54, no. 15, p. 2787–2805, 2010.

[2] N. K. M. P. B. T. M. N. a. A. O. H. Schaffers, "Smart cities and the future internet: Towards cooperation," *The Future Internet, Lect. Notes Comput.,* vol. 6656, p. 431–446, 2011.

[3] N. B. A. C. L. V. a. M. Z. Andrea Zanella, "Internet of Things for Smart Cities," *IEEE INTERNET OF THINGS JOURNAL,* vol. 1, no. 1, 2014.

[4] M. F. a. R. H. M. Hossain, "Towards an Analysis of Security Issues, Challenges, and Open Problems in the In-ternet of Things," in *IEEE 11th World Congress on Services* , New York, USA, 2015.

[5] L. D. R. Daniela POPESCUL, "Data Security in Smart Cities: Challenges and Solutions," *Informatica Economică,* vol. 20, 2016.

[6] D. Kushner, "The Real Story of Stuxnet. How Kaspersky Lab tracked down the malware that stymied Iran’s nuclear-fuel enrichment program," IEEE Spectrum, 26 February 2013. [Online]. Available: https://spectrum.ieee.org/telecom/secu-rity/the-real-story-of-stuxnet. [Accessed 28 October 2018].

[7] Z. S. F. W. H. H. K. L. F. G. I. B. a. C. X. Fu, "IPSec/VPN security policy: Correctness, conflict detection, and resolution," *Springer, Berlin, Heidelberg,* pp. 39-56, 2001.

[8] M. B. Leukert, "IoT 2020: Smart and secure IoT platform," IEC Market Strategy, Tokyo, 2016.