The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM)
ISSN: 2602-3199

The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM), 2019

Volume 7, Pages 249-252

IConTES 2019: International Conference on Technology, Engineering and Science

Cyber Security for Smart Cities

Murat DENER
Gazi University

Abstract: When the systems in smart cities are classified, there are generally eight categories. These are Smart Transportation, Smart Governance, Smart Economy, Smart Environment, Smart Health, Smart Industry, Smart Security, and Smart Life. There are dozens of intelligent systems in each category. The correct operation of these systems is as important as their security. For example, if any infiltration or intrusion into an intelligent system such as smart intersections, smart roads, crowd management, city noise mapping, smart energy, natural gas and water supply systems, early warning systems, the city may be in great danger. Natural disasters can be experienced as well as fatal consequences that affect human life. Therefore, the rulers of the smart city should always be on the alert and ensure the cyber security of the smart city. Cyber refers to electronic environments such as computer, server, device, hardware, software, protocol, algorithm, process, policy, process, laboratory, system. Cyber security is a set of methods, policies, concepts, and guidelines, risk management approaches, activities, trainings, best practice experiences and technologies used to protect the information assets of institutions, organizations and users. Intelligent strategies against cyber-attacks should be developed as the city environment created by smart systems has become very attractive for data thieves. Otherwise, a smart city can bring people closer to bad situations rather than bring people closer to technology. In this study, Cyber Security in Smart cities will be explained. The current literature review will reveal the latest trends in these two areas. The study is considered to be beneficial for smart cities technology developers.

Keywords: Smart city, Cyber security, Attack, Living, Technology

Introduction

A smart city infrastructure has many information systems such as fiber optic channels and wireless networks. Outer layers can be connected to the devices contained therein. Technologically, while these operations are performed, there is also a safety risk. In the city, there can be a power failure, water pollution, traffic incidents, material loss, loss of information, or even life-threatening.

Smart systems in smart cities have many parameters. These parameters can be either hardware or software. As examples, intelligent system forming sensor nodes, routers, gate nodes, embedded software, server required to send data detected by the gate node, database, cloud etc are given. Ensuring the high degree of security of these parameters is crucial for the safety of the smart city.

In this study, the current studies on cyber security in smart cities are shared with the elements of smart city.

Smart City

Smart city is the city where the technological opportunities for sustainable living and urbanization are implemented in the city and consequently economic, social and administrative benefits are provided. Some of the systems found in smart cities, as shown in Figure 1, are as follows.

Waste management, Electromagnetic Emissions, Smart Health, Education, Internet of Things, Smart Street Lights, Electric Vehicle Charging, Air Pollution, Smart Home, Smart Parking, Open Data, Public Safety, Smart

Environment, Smart Buildings, Traffic Management, Gas & Water Leak Detection, Intelligent Shopping, Smart Energy, Water Quality.

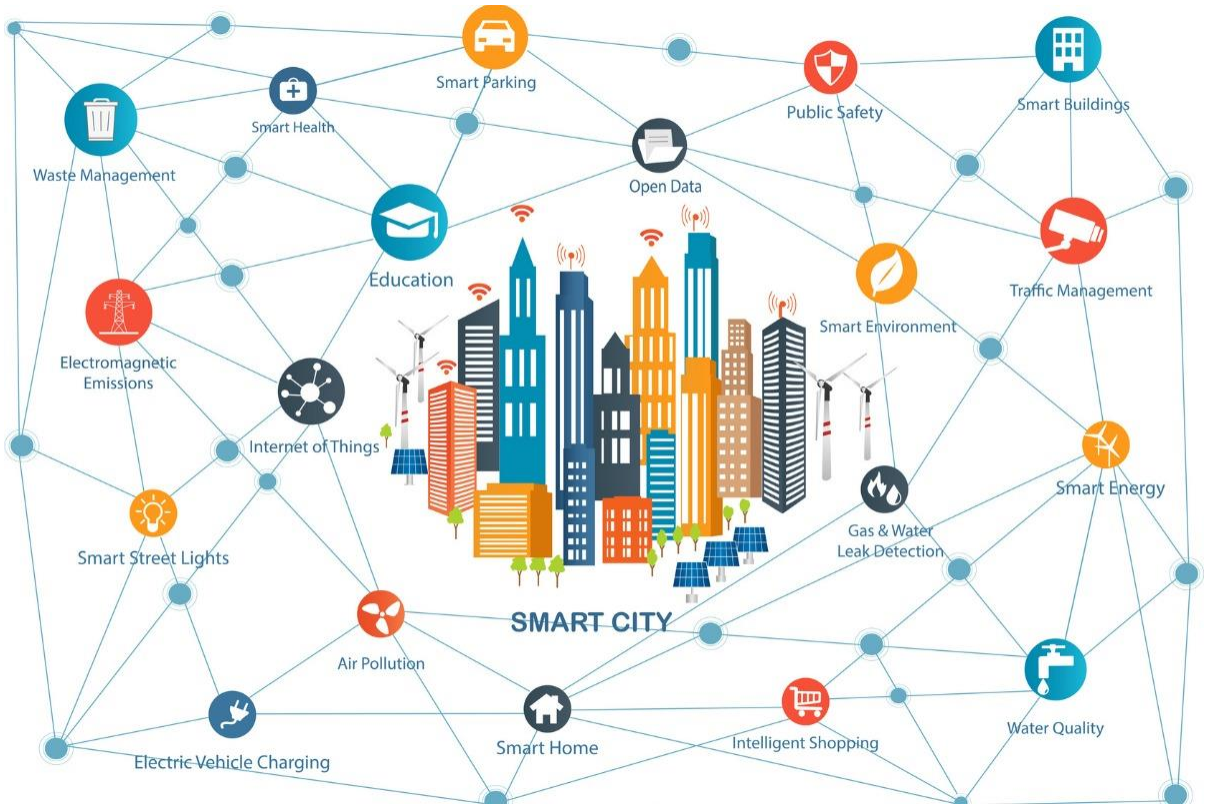

Figure 1. Smart City [SmartCitiesWorld news team, 2017]

Due to the increasing population density, cities may face many problems such as decrease in resources, pollution, increasing energy need and increasing communication need. The solution of these problems and the reduction of their effects is to make the city smart.

Cyber Security

Cyber refers to electronic environments such as computer, server, device, hardware, software, protocol, algorithm, process, policy, process, laboratory, system. Cyber security is a set of methods, policies, concepts, and guidelines, risk management approaches, activities, trainings, best practice experiences and technologies used to protect the information assets of institutions, organizations and users.

A smart city should have end-to-end protection to ensure cyber security. An attacker could infiltrate an existing vulnerability anywhere in the system and seize management.

All assets such as computers, smart devices, sensors, routers, network devices used in smart cities need to be protected. These protections must be both physical and software. Common technologies used to protect these assets include next-generation firewalls, DNS filtering, malware protection, antivirus software, and email security solutions.

Studies on cyber security in smart cities

When the literature is examined, it is seen that there are limited studies on cyber security in smart cities. These studies are described below.

In the study [Vitunskaite et al., 2019], 93 existing security standards related to smart cities were examined. Of the 93 security standards reviewed, 13 are related to cyber security. The security standards and security

measures of the smart cities of Barcelona, Singapore and London were analyzed. In addition, a new smart city security framework has been proposed.

As a threat in smart cities, a grouping is made as follows.

Threats from Intentional Attacks
Eavesdropping/wiretapping
Unauthorised use/access
Tampering/alteration
Theft
Malware/Virus
DDoS
Loss of Reputation

Threats from Accidents
Hardware failure/malfunctioning
Software error
Operator/User error
Electrical and frequency disturbance/interference
End of support
Acts of nature
Environmental incidents

The study [Parasol, 2018] reported that the Chinese government issued a law on the use of technology in the country. Due to the strict attitude of the published law, technology companies have become uneasy. There are also concerns that this law, which is prepared to protect China, will slow down China's technology. In this article, it is explained why China needs cyber security regime and the security law published by China is examined.

According to statistics from the Chinese state, the country has 731 million Internet users. Moreover, 695 million of them use the internet via their smart phones. According to the authors, this is one of the main reasons why China needs a security law.

The study [Baig et al., 2017] provides an in-depth insight into smart city security threats and digital investigation. In this study, four categories were identified as Smart Grids, Building Automation Systems, Unmanned Aerial Vehicles and Smart Vehicles and the technologies-platforms of these categories were shared. The security threats in these categories are given.

In the study [AlDairi and Tawalbeh, 2017], major security problems in smart cities and their valid solutions are given. In addition, it has been presented in many factors that affect data and information security in smart cities.

In the study [Elsaeidy et al., 2017], a new architecture has been developed for cyber attackers that affect the security of smart cities. In the architecture developed by using deep learning techniques, the behaviors of the users are taken into consideration.

The study [Wibowo, 2018] states that many smart cities in Indonesia have a web-based public services application. In order to test these services, a new method is proposed to measure the security level using the https evaluation method.

The study [Goel, 2015] examines the relationship between privacy and security and provides standards and guidelines for smart networks in smart cities.

In this study [Efthymiopoulos, 2016], smart city studies in Dubai have been given and together with these studies, necessary cyber security needs have been presented.

Conclusion

Ministry of Environment and Urbanization, Smart City concept within the scope of National Smart Cities Strategy and Action Plan 2019-2022; It is defined as a more livable and sustainable city, which is implemented

through inter-stakeholder cooperation, uses new technologies and innovative approaches, is justified on the basis of data and expertise and produces solutions that add value to life by anticipating future problems and needs.

Because smart cities are fully integrated with technology, cyber attackers can cause material, economic and even fatal losses from time to time. In order to prevent these losses, it is necessary to ensure end-to-end security of the city.

In order to ensure that the whole system is secure and not to leave any vulnerabilities at the security point, smart city security standards should be issued taking into account the standards developed by the public in the world (IEEE, ISO etc.).

Thus, each system installed in the city should be expected to meet these standards. Otherwise, a system that advances the city technologically can jeopardize the management and operation of the city due to the security gaps it contains.

References

AlDairi, A., Tawalbeh, L. (2017). Cyber Security Attacks on Smart Cities and Associated Mobile Technologies. *8th International Conference on Ambient Systems, Networks and Technologies (ANT-2017) and the 7th International Conference on Sustainable Energy Information Technology (SEIT 2017)*, 109, 1086-1091.

Baig, Z.A., Szewczyk, P., Valli, C., Rabadia, P., Hannay, P., Chernyshev, M., Johnstone, M., Kerai, P., Ibrahim, A., Sansurooah, K. (2017). Future challenges for smart cities: Cyber-security and digital forensics. *Digital Investigation*, 22, 3-13.

Efthymiopoulos, M.P. (2016). Cyber Security in Smart City of Dubai. *Proceedings of the 11th International Conference on Cyber Warfare and Security (ICCWS 2016)*, 107-118.

Elsaeidy, A., Elgendi, I., Munasinghe, K.S., Sharma, D., Jamalipour, A. (2017). A Smart City Cyber Security Platform for Narrowband Networks. *2017 27th International Telecommunication Networks and Applications Conference (ITNAC)*, 390-395.

Goel, S. (2015). Anonymity vs. Security: The Right Balance for the Smart Grid. *Communications of the Association for Information Systems*, 36, 23-32.

Parasol, M. (2018). The impact of China's 2016 Cyber Security Law on foreign technology firms, and on China's big data and Smart City dreams. *Computer Law & Security Review*, 34, 67-98.

SmartCitiesWorld news team. (2017). Smart cities services worth $225bn by 2026. Retrieved from https://www.smartcitiesworld.net/news/news/smart-cities-services-worth-225bn-by-2026-1618.

Vitunskaite, M., He, Y., Brandstetter, T., Janicke, H. (2019). Smart cities and cyber security: Are we there yet?A comparative study on the role of standards, third party risk management and security ownership. *Computers & Security*, 83, 313-331.

Wibowo, S. (2018). Enriching Digital Government Readiness Indicators of RKCI Assessment with Advance Https Assessment Method to Promote Cyber Security Awareness Among Smart Cities in Indonesia. *2018 International Conference on ICT for Smart Society (ICISS)*, 103-106.

Author Information

Murat Dener
Gazi University
Emniyet Mahallesi Abant-1 Caddesi No:10/2E Kat:8
06500 Yenimahalle / Ankara/Türkiye
Contact E-mail: *muratdener@gazi.edu.tr*