Mesopotamian journal of Cybersecurity
Vol.2022, **pp**. 1–4
DOI: https://doi.org/10.58496/MJCS/2022/001, ISSN: 2958-6542

Review Article

Cybersecurity Challenges in Smart Cities: An Overview and Future Prospects

Maad M. Mijwil[1,*], Ruchi Doshi[2], Kamal Kant Hiran[3], Abdel-Hameed Al-Mistarehi[4], Murat Gök[5]

1 Computer Techniques Engineering Department, Baghdad College of Economic Sciences University, Baghdad, Iraq
2 Department of Computer Science and Engineering, Universidad Azteca, Chalco, Mexico
3 School of Computer Science & IT, Symbiosis University of Applied Sciences, Indore, India
4 School of Medicine, Johns Hopkins University, Baltimore, Maryland, USA
5Department of Computer Engineering, Yalova University, Yalova, Turkey

ARTICLE INFO

Article History
Received 17 Dec 2021
Accepted 11 Jan 2022
Published 25 Jan 2022

Keywords
Cybersecurity
Smart cities
Internet of things
Artificial intelligent

ABSTRACT

Today, most governments in the world are considering establishing smart cities that work through the use of the latest technological means. Where smart cities are considered economically, socially and environmentally sustainable cities as they have the ability to develop sustainable development, increase the quality of life of citizens, increase the efficiency of available resources and active citizen participation with confidence and quickly. Nations are looking forward to creating a more profitable future for them by employing a set of main things, which are the economy, citizens, government, mobility, environment, and health. Smart cities are one of the main pillars that promote economic development in these nations. Smart cities have appeared in Japan, the UAE and Germany, where these cities constitute an excellent future environment in which they can live and are more suitable than ordinary cities. In this report, the most critical challenges that cybersecurity faces in preserving smart cities from hacking operations will be reviewed in general. This report concluded that there is a relationship between cybersecurity and smart cities. Such cities cannot be established without providing an appropriate electronic and physical security environment to protect these cities from attack and penetration by unauthorised or unknown individuals.

1. INTRODUCTION

The most influential factor that assisted build and development of smart cities is the growth of technologies and applications of artificial intelligence, the Internet of things, digitisation, and robots, as this development was mainly reflected like life and the various activities of man [1-3]. In addition, these factors helped create a new society that relies primarily on knowledge and digitisation, providing services with advanced virtual standards and getting rid of traditional measures that have become unwanted. Smart cities rely on artificial intelligence techniques, as these techniques collect information from the population and convert it into digital data in order to better understand and control all the operations carried out by the people and enhance the quality of services in these cities [4-5]. Moreover, these techniques seek to make a new generation of cities that rely on artificial intelligence in all its details because it provides appropriate, adaptable, practical, and scalable solutions. Artificial intelligence has entered many fields, including the sports field, where artificial intelligence is used in the FIFA World Cup currently held in Russia, where real-time offside detection techniques appeared. It is the first time that it is used through the use of inertial measurement unit (IMU) technology, which ensures the presence of a sensor in football. The elements of digital transformation have proven to be necessary and positive elements for intelligent cities, and at the same time, they may be harmful for them, because any error may be exploited and turned into threats and penetration through electronic attacks and cybercrime. Therefore, cybersecurity is necessary to control these attacks related to the misuse of digitisation and the electronic environment, and this is related to providing appropriate infrastructure and information systems based on artificial intelligence techniques, including machine learning and deep learning [6-8]. These techniques study the behaviour and practices of the electronic environment and detect anomalies in the systems while detecting intrusion and not allowing entry to people who do not belong to this environment. In general, cybersecurity is considered the shielding wall for the continuity of intelligent cities [9-10]. Smart cities are considered the new economic artery and modern sustainable development and seek to achieve a high quality of life of indulgence and safety [11]. The

*Corresponding author. Email: mr.maad.alnaimiy@baghdadcollege.edu.iq

United Arab Emirates seeks to develop smart cities and to apply artificial intelligence techniques in all fields. It even established a university for artificial intelligence called the Mohammed bin Zayed University of Artificial Intelligence. Therefore, all governments must enact and implement cyber laws with the spread of technology and communications in various economic, social, educational, medical, sports and other sectors. The existence of cyber laws regulating transactions between individuals and institutions generates a great feeling among users of safety in using technology and electronic services via the Internet [12-13].
The main contribution of this report is to review and highlight the importance of a cybersecurity field in protecting smart cities from electronic attacks, data and information theft, and intrusion detection. Cybersecurity aims to protect information and systems from threats large and small. These threats come in different forms, so cybersecurity operations represent a major challenge in controlling systems and data and protecting user information.

2. THE CHALLENGES

With the massive growth witnessed by the information revolution and the entry of the digital age in the twenty-first century, it caused the emergence of cybercrimes and threats that have become a significant threat to national security. Countless pieces of literature have emerged that consider cybercrime is the fifth domain in warfare after land, sea, air, and space. Therefore, the presence of cybersecurity is necessary to protect the digital environment. In this regard, the world is witnessing significant growth in technology, digital computing, and electronic devices, especially smartphones, and the transmission of information, which is considered one of the most important elements in the digital environment. It requires the existence of applications that protect the transfer of information and data, and that are documented and do not allow unauthorised individuals to enter this environment. These applications are characterised by the fact that they perform safely, as they preserve the privacy of people or institutions. Also, this digital growth has a negative influence on economic and commercial institutions, as it threatens to be hacked by crackers if it is utilised in the incorrect way or contains a security hole, as it can be exploited to control the systems within these institutions. Therefore, the existence of cybersecurity in smart cities is required to protect their data, networks, and electronic systems from attacks and breaches that threaten the stability of these cities.
Stealing sensitive data or information is one of the dreams of unauthorised individuals (hackers), modifying or deleting it, threatening people, or selling it to third parties. Thus, the term information security appeared, or what is named cybersecurity, which is a speciality that seeks to understand the different technologies and activities that people carry out to protect information systems and computer networks and not allow them to be tampered with and steal clients' data. In short, cybersecurity is the protection of things through information technology, such as hardware and software, where it takes a set of necessary measures to protect cyberspace from cyber-attacks, preventing illegal access to electronic information, irregularly preventing its exploitation, organising systems technically and administratively, and following the necessary procedures to protect data. Hence, cybersecurity concepts, purposes or definitions combine the national policy and technical dimensions by which cybersecurity is typically defined as protecting the confidentiality, integrity, and availability of computer systems data. Because such cyber-attacks, especially against critical information infrastructure, may threaten national security and people within the digital environment. The most important challenges facing cybersecurity in protecting information systems in the digital environment are:

- **Cyberspace:** It is an interactive environment that includes both physical and non-physical elements consisting of digital devices, network systems, software, and clients. This space seeks to link systems with the digital environment through the use of secure software and works under a registered corporate environment in order to secure interaction between customers in a digital environment free of malicious software. Here, the field of cybersecurity must provide a proper digital environment that is not vulnerable to attacks and entry of unauthorised individuals.
- **Cyber deterrence:** The digital environment must include a cyber deterrent against electronic attacks that exploit vulnerabilities in the systems and allow access to these systems, modify, and erase data, and add incorrect data, causing confusion or trouble in computer networks.
- **Cybercrime:** It is a set of illegal acts and acts that were carried out through a group of malicious software or electronic equipment installed inside the digital environment by individuals with experience in entering this environment and planting devices capable of dismantling the systems of the digital environment. Cybercrimes are activities that target computers to steal and manipulate content, which is prohibited.
- **Cyber-attacks:** It is the exploitation of vulnerabilities or loopholes that exist within computer networks intending to control the digital environment and threaten clients or institutions. The process of tampering with a system is one of the most critical challenges facing cybersecurity. It must focus on machine learning techniques that contain algorithms

capable of studying computer network data practices and training on them in order to be able to locate vulnerabilities and control them faster than hackers.

- **Cyber force:** It is the ability to control cyberspace and obtain data and information within the digital environment systems through the use of malicious software and illegal cyber tools.
- **Computer crackers:** They are a group of individuals who have the ability to manipulate computer systems in illegal ways. Their main purpose is to enter computer systems and gather information and data and manipulate or delete them. For instance, electronic theft of banks and, manipulation of customer funds, theft of social networking data. In fact, their goals are many; they seek to collect the most significant amount of information, create fake accounts and exploit clients.

Therefore, the existence of cyber security systems that support the objectives of the digital environment related to the effectiveness and efficiency of operations, issuance of reliable reports on all internal and external operations, and compliance with the laws and instructions in force within this environment. To protect smart cities requires the protection of information and the confidentiality of operations. However, cyber-attacks are repeated from time to time for a variety of reasons, including, for example: financial fraud, information theft or misuse.

3. CONCLUSIONS

Recently, technology has witnessed tremendous development in its applications, relying heavily on artificial intelligence techniques and the Internet of Things. In addition, it has a major and influential role in establishing smart cities and providing an infrastructure that guarantees systems that operate in a stable, secure, and devoid of loopholes. Artificial intelligence techniques are characterized by their ability to develop and keep pace with developments in the field of cybersecurity. Also, these techniques enhance countries' economic development and develop a digital environment that allows people to live in peace and security. In the coming years, the world will witness a great development in the establishment of smart cities and rely heavily on electronic services. The more digitisation processes increase, the more cyber-attacks will increase with them, which prompts countries to make great efforts to preserve these cities from these operations. Therefore, it is necessary to provide security for information technology systems and to provide the appropriate climate to protect smart cities and to set strong and strict laws and regulations for everyone who performs illegal operations in penetrating computer systems and networks. In the future, a piece of literature will be conducted on the importance of artificial intelligence techniques in the digital environment.

Funding

The authors affirm that this paper was entirely self-funded, and no financial support was obtained from any external organization or institution.

Conflicts Of Interest

The authors declare that there are no conflicts of interest related to the content presented in this paper.

Acknowledgment

The authors would like to express their sincere gratitude to all individuals who provided valuable insights and support during the preparation of this paper.

References

[1] A. Subeesh and C. R. Mehta, "Automation and digitization of agriculture using artificial intelligence and internet of things," Artificial Intelligence in Agriculture, vol. 5, pp. 278-291, 2021. [Online]. Available: https://doi.org/10.1016/j.aiia.2021.11.004

[2] B. P. L. Lau, S. H. Marakkalage, Y. Zhou, N. U. Hassan, C. Yuen, et al., "A survey of data fusion in smart city applications," Information Fusion, vol. 52, pp. 357-374, Dec. 2019. [Online]. Available: https://doi.org/10.1016/j.inffus.2019.05.004

[3] M. Kalinin, V. Krundyshev, and P. Zegzhda, "Cybersecurity Risk Assessment in Smart City Infrastructures," Machines, vol. 9, no. 4, pp. 1-19, Apr. 2021. [Online]. Available: https://doi.org/10.3390/machines9040078

[4] Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto, and K. Sakurai, "Towards a Lightweight Detection System for Cyber Attacks in the IoT Environment Using Corresponding Features," Electronics, vol. 9, no. 1, pp. 144, Jan. 2020. [Online]. Available: https://doi.org/10.3390/electronics9010144

[5] J. K. Lee, Y. Chang, H. Y. Kwon, and B. Kim, "Reconciliation of Privacy with Preventive Cybersecurity: The Bright Internet Approach," Information Systems Frontiers, vol. 22, pp. 45-57, Jan. 2020. [Online]. Available: https://doi.org/10.1007/s10796-020-09984-5

[6] M. Taddeo, T. McCutcheon, and L. Floridi, "Trusting artificial intelligence in cybersecurity is a double-edged sword," Nature Machine Intelligence, vol. 1, pp. 557-560, Nov. 2019. [Online]. Available: https://doi.org/10.1038/s42256-019-0109-1

[7] A. Khalifeh, K. A. Darabkh, A. M. Khasawneh, I. Alqaisieh, and M. Salameh, "Wireless Sensor Networks for Smart Cities: Network Design, Implementation and Performance Evaluation," Electronics, vol. 10, no. 2, pp. 1-28, Jan. 2021. [Online]. Available: https://doi.org/10.3390/electronics10020218

[8] D. Chen, P. Wawrzynski, and Z. Lv, "Cyber security in smart cities: A review of deep learning-based applications and case studies," Sustainable Cities and Society, vol. 66, pp. 102655, Mar. 2021. [Online]. Available: https://doi.org/10.1016/j.scs.2020.102655

[9] A. L. Karn, S. Pandya, A. Mehbodniya, F. Arslan, D. K. Sharma, et al., "An integrated approach for sustainable development of wastewater treatment and management system using IoT in smart cities," Soft Computing, pp. 1-17, Sep. 2021. [Online]. Available: https://doi.org/10.1007/s00500-021-06244-9

[10] C. Kim and K. Kim, "The Institutional Change from E-Government toward Smarter City; Comparative Analysis between Royal Borough of Greenwich, UK, and Seongdong-gu, South Korea," Journal of Open Innovation: Technology, Market, and Complexity, vol. 7, no. 1, pp. 1-33, Jan. 2021. [Online]. Available: https://doi.org/10.3390/joitmc7010042

[11] C. S. Lai, Y. Jia, Z. Dong, D. Wang, Y. Tao, et al., "A Review of Technical Standards for Smart Cities," Clean Technologies, vol. 2, no. 3, pp. 290-310, Aug. 2020. [Online]. Available: https://doi.org/10.3390/cleantechnol2030019

[12] H. Albayati, S. K. Kim, and J. J. Rho, "Accepting financial transactions using blockchain technology and cryptocurrency: A customer perspective approach," Technology in Society, vol. 62, pp. 101320, Aug. 2020. [Online]. Available: https://doi.org/10.1016/j.techsoc.2020.101320

[13] R. H. Weber and E. Studer, "Cybersecurity in the Internet of Things: Legal aspects," Computer Law & Security Review, vol. 32, no. 5, pp. 715-728, Oct. 2016. [Online]. Available: https://doi.org/10.1016/j.clsr.2016.07.002