A Systematic Literature Review on Cybersecurity Risk Management in Smart Cities

Jawaher Alshehri, Almaha Alhamed , M M Hafizur Rahman
Department of Computer Networks & Communications.
King Faisal University, College of Computer Science and Information Technology
Al Hofuf, Al Hassa 31982, Saudi Arabia,
223001719@student.kfu.edu.sa , 223000349@student.kfu.edu.sa , mhrahman@kfu.edu.sa

***Abstract*—A smart city is a digital and intelligent city that uses communication and information technology (ICT) that contains different types of technology methods to meet the needs of current and future generations regarding economic, social, cultural, and environmental aspects. Smart cities face many risks in technology, which make their management difficult and easy to attack. The concept of smart cities has emerged as a promising solution to face various urban challenges. In addition, it has been determined that a 38.7 percent increase in smart city risk management significantly increased the number of attacks across the TOE (technology, organization, and environment) categories. The research aims to highlight the role of cybersecurity risk management in smart cities, including preventing threats and the essential attacks that face smart cities. To strengthen the security and resilience of smart cities, it is crucial to comprehend the unique difficulties and dangers related to cybersecurity in these urban environments and take necessary steps accordingly. The primary objective of this research is to enhance the cybersecurity risk management role in smart cities, thereby guaranteeing the sustainable and secure growth of technologically sophisticated metropolitan regions. Index Terms—Cybersecurity risk management, smart cities,risk management , internet of things (IoT), artificial intelligence.**

***Index Terms*—Cybersecurity risk management, smart cities ,risk management ,internet of things , artificial intelligence**

I. Introduction

Smart cities have significantly increased in number as a result of the recent rapid expansion of technological development. The smart city concept uses ICT to increase the comfort and livability of urban life while also making services more effective. The United Kingdom, China, and Hong Kong are the most notable nations to have embraced smart city technologies [1]. Recently, Saudi Arabia began implementing smart city projects such as NEOM and THE LINE, which will help the country realize its 2030 vision. According to a prior study, 135 billion dollars will be spent by 2024 on smart city cybersecurity, and 1.3 billion digital service infrastructures will be present in smart cities[2]. The most significant challenge in developing smart cities is the technical challenge, despite the socioeconomic and political challenges they face. The worry of security and privacy in technical challenges is essential; threats have always been a challenge for smart cities to thwart. Therefore, it is essential to implement risk management to minimize the effects of dangerous threats, particularly those that may be intensified by recent technological advancements such as artificial intelligence (AI) and the internet of things(IoT) [3]. As Fig 1 shows, cybersecurity risk management covers three main areas: AI, IoT, and ICT, which use their technology in smart city infrastructure. AI refers to machines or systems that perform tasks similarly to human intelligence and can iteratively improve themselves based on the information they gather. IoT refers to the overall network that connects devices as well as the technology that permits communication between those devices and the cloud that resides inside each one of them. ICT is the umbrella term for a variety of technological tools and resources used to produce, transmit, store, share, and exchange information. A strategic approach is to prioritize threats through cybersecurity risk management. For instance, organizations use cybersecurity risk management to make sure that the majority of threats are addressed quickly. This technique assists in identifying, analyzing, evaluating, and mitigating threats based on the potential harm each threat may cause. This research will emphasize the significance of cybersecurity risk management in smart cities and show some of the techniques used in smart cities that play a role in risk management in order to lessen threats and the most serious attacks that smart cities face.

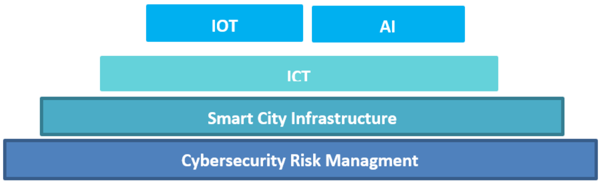

Fig. 1. Cybersecurity Risk Management Covering

II. Selection of papers for literature review

In the current paper, PRISMA is one of the research techniques utilized. It supports identifying and minimizing redundant research on smart city cybersecurity risk management. The definition of research studies and papers using PRISMA involves a few steps. The first step is to conduct a Google Researcher and Saudi Digital Library search using the keywords ”cybersecurity risk management AND smart cities,” ”risk management smart cities” AND ”cybersecurity smart cities,” ”smart city challenges” AND ”risk assessment in smart cities,” and ”smart city risk analysis” AND ”cyberattack smart cities.” In the second step, some criteria are defined, with a particular emphasis on studies on the significance of cybersecurity risk management in smart cities and papers published between 2016 and 2022 .

Fig2: Prisma-based schematic diagram for managing cybersecurity risk in smart cities. The initial outcome was that the Saudi Digital Library and Google Scholar databases were able to identify 470 papers. In addition, we identified 245

duplicate studies prior to 2016. We eliminated 100 of the 225 remaining studies because they did not meet our research objectives. We excluded 100 research papers in the final step. After reading the introductions and arguments for each, we accepted 25 research papers.

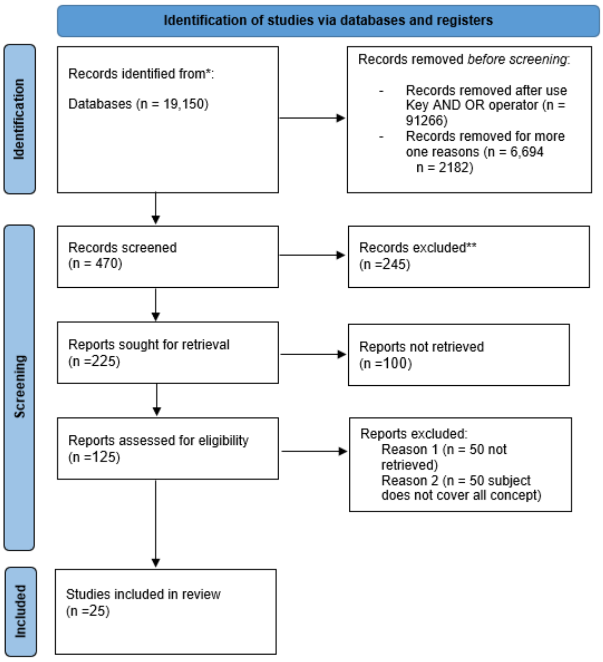
Identification of studies via databases and registers
Identification
Records identified from*:
Databases (n = 19,150)
Records removed *before screening*:
- Records removed after use Key AND OR operator (n = 91266)
- Records removed for more one reasons (n = 6,694 n = 2182)
Screening
Records screened (n = 470)
Records excluded** (n =245)
Reports sought for retrieval (n =225)
Reports not retrieved (n =100)
Reports assessed for eligibility (n =125)
Reports excluded:
Reason 1 (n = 50 not retrieved)
Reason 2 (n = 50 subject does not cover all concept)
Included
Studies included in review (n =25)

Fig. 2. PRISMA cybersecurity risk management In smart cities.

III. Literature Review

This section reviews 25 papers on smart city risk management in terms of an overview and findings of some of the methodologies and technologies used in smart city protection and management in smart transport, health, environment, and living. These methods and models provide solutions to the challenges faced in smart city systems and risk assessment. They detect deviations and abnormalities that can be utilized in various contexts to ensure smart city security. Further, the most used technology in smart cities plays a role in protecting against risk and threat.

Ref	**Year**	**Framework or approach used**	**Contribution**
[1]	2020	•Used some security techniques to avoid risk in smart cities (access control. • Multi-factor authentication, encryption, end point protection. • Blockchain for protection of financial transactions .	This paper provides an overview of risk assessment by exploring the potential risks that affect smart cities, including some threats and best practices that can be applied in smart cities, which can be seen as a protection approach to risk management.
[2]	2021	• Artificial neural networks for risk assessment in smart cities	The paper explores the challenges of traditional risk assessment methods in smart cities. It suggests the use of artificial neural networks for more effective risk assessment. Also present a neural network model for identifying and assessing cybersecurity risks in dynamic networks.
[4]	2022	• NIST •Integration of Assurance Standards •Systems-Based Approach	Discuss the role of cybersecurity risk management in smart cities and explore some of the approaches used to risk assessment.
[5]	2020	• Risk Assessment Models • Cognitive Security Techniques	The paper highlights the importance of estimated risk assessment and management of cybersecurity in smart cities; they suggest confining security techniques to evaluate cybersecurity risk levels; they also discuss the development of cybersecurity procedures by third parties; and the need for security to be included in IoT solutions from the design stage.
[6]	2020	• RiskLens • FAIR	The paper discusses the role of cyber security in risk management; it covers some of the threats in the IoT system, which is considered part of smart cities. It mentions some of the methods used in cybersecurity risk management, such as FAIR and RiskLens.
[7]	2020	• Linear Programming (LP) model	Linear Programming model (LP) is model used in this paper for cybersecurity risk management to allocation of limited resources, such as financial resources, among competing IoT cybersecurity projects.
[8]	2022	• Attack-defense trees (ADTs)	Analyze the attack-defense trees (ADTs) strategy as a response to problems in smart city systems by putting forth a continuous quantitative risk management methodology for intricate smart grid systems that coordinate many components.

Ref	Year	Framework or approach used	Contribution
[8]	2022	• System of Systems (SoS) approaches	This paper presents a system of system model SOS ,that plays a role in management smart cities from risk. It studies the risks that affect smart cities and used the SOS model to manage risk and city governance.
[9]	2020	• Attack-defense trees (ADTs)	Analyze the attack-defense trees (ADTs) strategy as a response to problems in smart city systems by putting forth a continuous quantitative risk management methodology for intricate smart grid systems that coordinate many components.
[10]	2021	•Establishing information security policies and control measures	discusses cybersecurity risk management in smart cities, highlighting the vulnerability of these systems to cyberattacks due to the integration of diverse technologies. It confirmed the need for measures such as network intrusion detection, information security policies, access control, auditing, activity logs, and backup maintenance.
[11]	2019	Normative approach	The paper advocates for a normative cybersecurity risk management approach in smart cities, in term of systemic interventions like security-remedial patching, by-design, procurement , core security teams, changes, and professional development.
[12]	2021	• Present lot of models used in risk assessment threats in smart cities	The methods used for risk assessment in smart city attacks, deviation and abnormality detection, and system state comparison are the main topics of this paper, which is play role in detection risk and assessment.
[13]	2021	• Present a lot of methods and theory for risk assessment in smart cities.	The development of a general, planner-oriented methodology to evaluate risk for planning inputs for smart cities is the main driving force behind the research; risk assessment methodologies that can be applied in various contexts are mentioned.
[14]	2022	Used tools for risk assessment and management	This study includes a review of the literature to look into risk management and assessment tools and methods. for smart cities, as well as the most recent technological advancements. The paper's conclusion discusses the potential for further research into risk assessment instruments for a smart city implementation project.
[15]	2021	• TOE	A multilayered framework for risk management based on the technology organization environment (TOE) is proposed by research for sustainable smart city governance.
[16]	2020	• Smart Cities Security & Privacy Framework	This paper explores privacy, security, and risk challenges in smart cities, proposes a framework for managing cybersecurity risks, and discusses current knowledge on these topics.
[17]	2022	• Methodology to assess and rank Smart Cities	This study's goal is to suggest a methodology for assessing Smart Cities utilizing a multi criteria approach, as this approach is suggested for dealing with complicated issues that involve competing interests.
[18].	2020	• Used assessment tools for smart city	This paper is focused on the assessment tools for smart city implementation evaluation, which can also be mentioned as smart city assessment (SCA).
[19]	2021	Smart city security issues: The main attacks and countermeasures	Highlighting its main applications and services for smart cities, presenting some susceptible attacks that can touch the security of applications, and some best practices to ensure smart city security.

Ref	Year	Framework or approach used	Contribution
[20]	2021	• AI methods	The study addressed detecting an attack on IoT by using artificial intelligence, deep learning, and machine learning to safeguard IoT, which is the most used technology in smart cities and plays a role in protecting from risk and threat.
[21]	2022	• Using cybersecurity and failures in telecommunication infrastructure . • Multidisciplinary approach	The purpose of this paper was to specify the risks of smart cities and the perspectives of risk management and lies in the description of a new angle of studying smart cities.

IV. Methodology

Cybersecurity risk management plays an important role in ensuring the security and resilience of smart cities. It involves the identification, assessment, and mitigation of potential cybersecurity risks that may establish due to the implementation of advanced technologies in urban environments. Cyber incidents can still happen in spite of mitigating actions. Building strong incident response skills is just one aspect of cybersecurity risk management's responsibilities. This entails creating incident response strategies, educating staff, and putting systems in place to efficiently identify, address, and recover from cyber events. This section will highlight the most important threats that affect smart cities and their countermeasures, such as the activities in IoT-based smart cities, privacy issues with virtual reality, and issues with smart cities and the dangers that AI presents in them [22]. Additionally, presenting some of the techniques and strategies that cybersecurity risk management depends on to protect and secure the infrastructure to be more secure and hard to access.

Some problems affecting smart cities and their solutions will be covered in this part, including risks posed by driverless automobiles, privacy concerns with virtual reality, and botnet activity in Internet of Things-based smart cities. Furthermore, outlining some of the methods and approaches that cybersecurity risk management uses to protect and secure the infrastructure in order to make it more difficult to access and safe [22].

A. *The most issues in smart cities*

1) IoT-based smart cities botnet activities: Mirai Bonten is the most common threat that infects devices such as cameras, printers, routers, and DVRs. It propagates infection to a large number of diverse IoT devices and launches a DDoS attack against target servers [22]. Secure and agile SEAL is one of the frameworks that is being used to detect and mitigate DDOS attacks on smart city applications and network infrastructure. It was especially created to address the adaptability requirements of smart city applications, thus providing effective defense against DDoS attacks for smart city applications. The SEAL framework provides various types of filters to satisfy application-specific security requirements. (Proactive Filter, Active Filter, and Passive Filter). One can alter these filters to achieve the crucial accuracy required for attack detection. The benefits of using the SEAL framework to defend against DDOS attacks for all services and applications, not just specific ones in smart cities [23].

2) Driverless car threats in smart cities: Autonomous vehicles (AVs) are designed to lessen traffic and create a modern, environmentally friendly society. Using the steering wheel, slamming on the brakes, or turning off the engine are just a few of the extremely dangerous threats you might be exposed to. Along with violating privacy by stealing or losing information [22], An autonomous vehicle's operating system—and potentially the entire network—can be accessed by an attacker by simply taking advantage of one vulnerability within the system. Because autonomous vehicles are so complicated, certain experts believe that they may never be completely secure. However, there are definitely ways to increase the security of autonomous car technology. Manufacturers, cities, and drivers may protect autonomous cars in six different ways, including Set up a special passcode, Instead of just one network, cities should implement several. In addition to turning off GPS and updating the vehicle's software.

3) Virtual reality privacy issues in smart cities: Smart cities depend on technology. one of those used technologies is virtual reality. Different organizations have embraced virtual reality (VR) technology in smart cities such as the engineering industrial and healthcare sectors. However, the sensitive information that had been shared in any possible way or unencrypted connections between virtual reality devices and others, all of that is affecting and posing some threats to privacy by leakage or interfering with it. [22] Unfortunately, this case is still confusing the designers and users in taking any appropriate decisions to protect and countermeasure privacy. However, there are some countermeasures that may help to protect such as using "privacy by design" principles and implementing the hidden identity. By taking these steps, smart cities can ensure using the data for legitimate purposes and protect individuals' privacy. [24]

4) Threats AI pose in smart cities: The most important roles in various smart applications, particularly in smart cities, are played by artificial intelligence systems. However, the growing use of AI creates dangers and security risks. Service providers, for instance, may employ certain techniques to extract data, analyze personal data in excess, and extract sensitive information that goes beyond service-providing objectives and grants unauthorized access to data. Hackers can weaken the effects of training and reduce the accuracy of the algorithm because they are aware of how ML-based defenses were developed or trained. Organizations can use some of the techniques of artificial intelligence to improve while taking precautions [22]. AI identifies unknown threats: a large number of hackers every year and significant numbers of attacks with several motives. These unknown threats may cause huge damage to networks. For decreasing the problem, Al is considered one of the best techniques to prevent these threats and discover unknown threats. Finally, secure authentication: most websites contain user accounts that are individual logins for accessing required services. Organizations need an extra layer to protect the sensitive and personal information of their users. However, AI secures the authentication anytime users want to log in to their accounts. AI uses a lot of tools, including fingerprint scanners and facial recognition, which help detect the number of hack attempts.[25]

B. *Techniques and Strategies*

1) Smart cities infrastructure: cybersecurity risk management depends on an object type, extracting data and evaluating quantitative risk for the infrastructure in smart cities. The most famous smart city technologies that face attacks and technical problems with a large percentage are the internet of things (IoT) technique and the artificial intelligence (AI) technique. Artificial neural networks allow for assessing cyber risk in the infrastructure of different types of objects in the dynamic digital infrastructures of the smart city [2]. In disaster cases, the infrastructure face also has some challenges in avoiding any electronic problems that may cause by natural phenomena. So, an integrated resilience system is connected with a smart city to improve disaster resilience by using artificial intelligence technology [4]. The more robust and solid the infrastructure, the more protection the risk management will be.

2) Disaster management: A decision support system that deals with the infrastructure that will support a disaster. management system in the smart city. The smart city needs to be prepared for disasters, adapt to them, and respond to and recover from them by taking the benefits from the links. between the different infrastructures to increase resilience to any disaster they face [4]. This will help risk management to prepare for any disaster cases.

3) Role of risk management : The effectiveness of smart cities depends on the risk management approach for protecting them from threats or cyberattacks that may affect their efficiency and discontinue their work, which results in the possibility of losing important data and material and technical resources, which affects the economic aspect of cities. Risk management requires the creation of systematic strategies based on the structuring of smart cities. They are also using new technologies that are increasing productivity. and work effectively. The risk management procedure consists of five steps: risk identification, analysis, and evaluation. , treatment, and monitoring. The purpose of risk identification is to determine what, where, when, why, and how something might impair operations. Establishing the likelihood of a risk event and the possible results of each event are both part of the risk analysis process. Each risk's relative magnitude assessed, and risks are then categorized according to their importance and impact. In this step, risk management strategies, preventative measures, and contingency plans developed based on the estimated value of each risk. Risk management is a dynamic, ongoing process that includes risk monitoring. Regular repetition and observation of the procedures aid in ensuring that both anticipated and unanticipated risks are fully addressed.

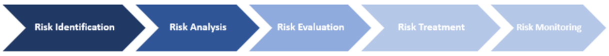

Fig. 3. Cybersecurity risk management framework

4) Technology organization environment framework (TOE): Risk management for smart cities employs a variety of frameworks and theories. Contrary to TOE frameworks, which offer a more comprehensive approach from the three sides of technology organization environment, the majority of them do not cover the environmental and organizational aspects of smart cities. The TOE framework evaluates, monitors, and regulates the risks connected to various processes and their integration into the overall management of smart cities. The proposed architecture for smart cities layers iterative risk management and TOE processes to provide for comprehensive city administration.

5) IoT models in the smart city: In smart cities, the internet of things (IoT) is the most significant and widely used technology. The majority of cyberattacks on smart cities have an IoT component. In order to improve smart cities, cybersecurity risk management focuses on a few models. It identifies a Bayesian model to assess cybersecurity maturity, which is crucial support for enhancing cybersecurity at the level of smart cities and guaranteeing their functionality[5]. In the IoT and IoMT domains, a novel IoT risk computational model also computes the potential risk and risk effect score [6]. Additionally, an LP model is created to decide how to divide resources among several IoT security projects that are in competition with one another [7].

6) Attack defense trees: Attack defense trees are models used to evaluate system risks by including risk attributes in the tree nodes. We can perform some sensitivity analysis of system risks relating to defenses and attacks using this technique, which also allows us to enhance safety measures for facilitating risk management and lowering risks [9].

7) The Security and privacy: Devices are seen as brand-new threats to user security and privacy because they put confidential data at risk of attack by a third party. To safeguard the user's privacy, the idea of foggy dummies was used. Other hazy methods for reducing security risks in cybersecurity risk management included caching, cooperating, and serving as a middleman between users [16].

V. Recommendations and Future Directions

This research covered a comprehensive and general overview and analysis of some strategies and methodologies used in risk management in smart cities. Risk management is important for any organization and any country, especially with this generation, which is increasingly adopting technology in all dealings, whether in education, health, home, companies, etc. This research focused mainly on risk management in smart cities because of their great diversity and the orientation of most countries toward them. With the increase in technologies used in them, the risks increase and thus may affect the quality of human life and the economies of countries as well. It analyzed some of the methodologies used in previous research and clarified the contributions of each, in addition to mentioning some of the threats and means of protection used. It is considered a broad and complex field and requires more experiments, research, and contribution to focusing on creating strong means of protection and management of cyber risks that may affect smart city devices and systems.

In this research, we propose creating a special smart city platform that contains all the devices and departments in smart cities, which makes it easier for developers and technicians to manage this specific city. The platform includes smart city departments; for example, the health department is separate from the education department, and so on, and each department contains the number of devices and systems used for each device. This platform also reviews the behavior and results of these devices, the rate of hacking attempts, and their proccessing . Which means that this platform displays results and numbers for everything contained in smart cities, to makes it easier for managers and technicians to find results, evaluate risks, and make decisions as well through this platform. This proposal will contribute to collecting and understanding all the information we need to manage a smart city on one platform, which will raise the quality of risk management and able to decision-making based on the presented results. On the other hand, it requires a lot of effort and collecting all the information, which takes a long time, in addition to features that are added to this platform, such as issuing reports, clarifying graphs in it, etc., to raise the quality of its use.

VI. Conclusion

At this time, with growing information technology and communications related to the economy of countries in all fields such as health care, education, and transport .etc, it becomes some of the countries transfer to be as smart cities, and It is closely connected with IT and communications. The smart city continuously faces risks; the more significant the smart city, the greater its risks. Since the smart city has different factors of risks, this study sought to highlight the vital role of cybersecurity risk management in smart cities in terms of technologies used and infrastructure that consider essential factors in managing the risk.

References

[1] Toh, C. K.: Security for smart cities. IET Smart Cities. 95-104 (2020)

[2] Kalinin, M., Krundyshev, V., Zegzhda, P.:Cybersecurity risk assessment in smart city infrastructures. Machines, 9(4), 78 (2021)

[3] Ijaz, S., Shah, M. A., Khan, A., Ahmed, M.: Smart cities: a survey on security concerns.(IJACSA) Int. J. Adv. Comput. Sci. Appl, 7(2) (2016)

[4] Chaudhuri, A., & Bozkus Kahyaoglu, S.: CYBERSECURITY ASSURANCE IN SMART CITIES: A RISK MANAGEMENT PERSPECTIVE. EDPACS, 67(4), 1-22. (2023)

[5] Andrade, R. O., Yoo, S. G., Tello-Oquendo, L., Ortiz-Garces, I.: A comprehensive study of the IoT cybersecurity in smart cities. IEEE Access, 8, 228922-228941 (2020)

[6] Kandasamy, K., Srinivas, S., Achuthan, K., Rangan, V. P.: IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. EURASIP Journal on Information Security, 1-18 (2020)

[7] Lee, I.: Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. Future Internet, 12(9), 157 (2020)

[8] Nguyen, T., Hallo, L., Nguyen, N. H., Pham, B. V.: A Systemic Approach to Risk Management for Smart City Governance.IEEE 978-1-6654-8371-1 (2022)

[9] Rios, E., Rego, A., Iturbe, E., Higuero, M., Larrucea, X.: Continuous quantitative risk management in smart grids using attack defense trees. Sensors, 20(16), 4404 (2020)

[10] Saber, O., Mazri, T. : Smart City Security Issues: The Main Attacks and Countermeasures. The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, 46, 465-472

[11] Sabou, G. C., Maiorescu, I.: Cybersecurity challenges in Smart Cities–a Smart Governance Perspective (2020)

[12] Mohammadi, F.: Emerging challenges in smart grid cybersecurity enhancement: A review. Energies, 14(5), 1380 (2021)

[13] Al Sharif, R., Pokharel, S.:Risk Analysis with the Dempster–Shafer Theory for Smart City Planning: The Case of Qatar. Electronics, 10(24), 3080.(2021)

[14] Al Sharif, R., Pokharel, S.:Smart City Dimensions and Associated Risks: Review of literature. Sustainable Cities and Society, 103542. (2021)

[15] Ullah, F., Qayyum, S., Thaheem, M. J., Al-Turjman, F., Sepasgozar, S. M.: Risk management in sustainable smart cities governance: A TOE framework. Technological Forecasting and Social Change, 167, 120743 (2021)

[16] Ismagilova, E., Hughes, L., Rana, N. P., Dwivedi, Y. K.: Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. Information Systems Frontiers, 24(2), 393-414 (2022)

[17] Chiroli, D. M. D. G., Solek, É. A., Oliveira, R. S., Barboza, B. M., Campos, R. P. D., Kovaleski, J. L., ... Trojan, F.: Using multi-criteria analysis for smart city assessment. Cidades. Comunidades e Territórios, (44). (2022)

[18] 18. Patrão, C., Moura, P., Almeida, A. T. D.: Review of smart city assessment tools. Smart Cities, 3(4), 1117-1132.(2020)

[19] Saber, O., Mazri, T.: Smart City Security Issues: the Main Attacks and Countermeasures. The International Archives of Photogrammetry, Remote Sensing and Spatial Information Sciences, 46, 465-472 (2021)

[20] Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L. F., Abdulkadir, S. J.: Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review. Electronics, 11(2), 198 (2022)

[21] Morozova, I. A., Yatsechko, S. S.: The Risks of Smart Cities and the Perspectives of Their Management Based on Corporate Social Responsibility in the Interests of Sustainable Development. Risks, 10(2), 34. (2022)

[22] Cui, L., Xie, G., Qu, Y., Gao, L., Yang, Y.: Security and privacy in smart cities: Challenges and opportunities. IEEE access, 6, 46134-46145 (2018)

[23] Bawany, N. Z., Shamsi, J. A.: SEAL: SDN based secure and agile framework for protecting smart city applications from DDoS attacks. Journal of Network and Computer Applications, 145, 102381 (2019)

[24] Nasralla, M. M.: Sustainable virtual reality patient rehabilitation systems with IoT sensors using virtual smart cities. Sustainability, 13(9), 4716 (2021)

[25] Jakka, G., Yathiraju, N., Ansari, M. F.: Artificial Intelligence in Terms of Spotting Malware and Delivering Cyber Risk Management. Journal of Positive School Psychology, 6(3), 6156-6165 (2022)