MAIKRON

Journal
of
Artificial Intelligence
and
Computing Applications

Review article

Challenges in network security for smart cities: a short narrative review

Gadiel Antonio Sosa-Chan[1], Bryan Emmanuel Puc-Diaz[1], Jhonatan David Arcila-Choc[1], José Antonio Cicero-Osorio[1], and Roberto Daniel Gonzalez-Lopez[1]

[1]Tecnológico Nacional de México / IT de Mérida, Yucatán, México

ABSTRACT

It is estimated that smart cities invest in the development of new technologies to improve the quality of life for citizens. By implementing these new technologies, issues of security and privacy have become a relevant challenge for the development of smart cities. Implementing traditional cybersecurity strategies to address these issues becomes obsolete, as contemporary threats are more complex. Motivated by these factors, we examine the current challenges, vulnerabilities, and threats present in smart cities regarding privacy and data protection to determine how these issues affect smart cities and their citizens. We begin this article with a description of the current situation of smart cities. Next, a compilation and selection of literature were carried out for the completion of this work, following certain selection criteria to obtain 20 articles. We then analyze the most recent challenges and threats regarding privacy and security present in smart cities. Subsequently, threats and challenges were compiled with a focus on how they affect smart cities and their citizens. Finally, we present gaps for future research and identify directions for future investigations.

Keywords: network security, smart cities, threats and vulnerabilities

1. Introduction

Nowadays, the term *smart city* is becoming increasingly crucial in response to the growth of the urban population. It is estimated that by the year 2050, almost two-thirds of the population will reside in smart cities [1]. Although the precise definition of a smart city is somewhat complex, it generally refers to places that invest in technology to improve the quality of life for residents, with the government playing a key role in managing natural resources [2]. In this modern context, smart cities have emerged as places where technology defines the way we live. These advanced urban centers seek to enhance efficiency, sustainability, and, above all, well-being. However, challenges to the development of smart cities exist, and one of the most prominent issues is network security, especially concerning security and privacy.

Security is not the only challenge for the development of smart cities; economic factors also come into the game. This has led to a decrease in investments in public services in such projects, hindering the flourishing of these cities in many cases [3]. The implementation of this smart urbanization faces various issues, including cyber attacks, mishandling of information, Denial of Service (DOS), and vulnerabilities in connected devices that are part of the cities' networks, known as the Internet of Things (IoT). These vulnerabilities are often linked to data collection and third-party service providers [1], posing significant risks in the smart urban environment. In addition to threats derived from data collection, there are potential attacks that can directly damage network infrastructure, such as Distributed De-

E-mail address: le23081226@merida.tecnm.mx

https://doi.org/10.5281/zenodo.10420999

nial of Service (DDoS) attacks [4], among many other vulnerabilities that greatly affect smart cities and their citizens.

However, there is an urgent need to update information on the challenges and cybersecurity threats present in smart cities. This need is based on the crucial importance of understanding these challenges to develop strategies and solutions, thus driving the progress of smart cities.

The purpose of this article is to review the literature and present an updated analysis of the most prominent and sophisticated cybersecurity threats, vulnerabilities, and challenges in smart cities. Given the recent advances in these urban areas, it is crucial to understand the cybersecurity risks affecting both infrastructure and citizens. In response to the challenges posed, we have formulated key questions to address these issues. We aim to explore in detail questions such as: What are the most prominent and advanced threats and vulnerabilities facing IoT networks in smart cities? Furthermore, how do these threats affect the security of citizens? These questions will be analyzed to gain a deeper understanding of the vulnerabilities and threats facing smart cities.

In the review, we highlight four key sections that we address: in Section 2, we define the parameters that guided our article selection; in Section 3, we broadly cover the central ideas of the established literature; in Section 4, we delve more specifically into the development of these key ideas; and finally, in Section 5, we summarize the ideas and justify the importance of compiling this information.

2. Methodology

In this section we describe the selection process, including our inclusion and exclusion criteria. We utilized Google Scholar and Semantic Scholar as our main search engines, recognized for their extensive repository of academic articles in various disciplines, including the field of computer science. These platforms were selected for their comprehensive indexing, search capabilities, user-friendliness, and integration with a wide range of academic journals from different years, making them highly suitable for conducting an extensive and high-quality literature search.

We initiated our search with a set of keywords such as "Network security", "Smart city", "Network security challenges", "Smart security", and "Security for smart home", with the aim of gathering key information for our review. Our inclusion criteria were strict to ensure a high standard of quality and relevance. Each co-author undertook a thorough process to select the articles that would form the basis of our review.

In the initial phase of article searching, we encountered a considerable volume of literature (126 articles) that required careful organization and filtering by the co-authors. To carry out the exclusion process, we used the Mendeley management tool. On this platform, we conducted a thorough review and verification of duplicates, ensuring the uniqueness of each article. After this process, we obtained a total of 91 articles. In the same way, we used the same tool for detailed reading and inquiry of each document. We limited our scope to articles published between 2014 and 2023, ensuring contemporary knowledge. This left us with 77 articles. Continuing the literature reduction process, we focused solely on articles published in English, reducing our literature to 70 articles. Furthermore, we limited ourselves to journals indexed in the Journal Citation Reports (JCR), specifically those classified as Q1, representing superior quality in the field. However, in the presence of highly relevant information, we were willing to make exceptions, allowing the inclusion of a Q4 article, leaving us with 53 articles. Additionally, we focused on original research articles and reviews, resulting in 43 articles. Considering quality, we aimed for coverage of minimum 10 cites per year, discarding 11 articles. Finally, we conducted an initial reading, allowing us to discard articles that did not fit correctly with the theme of the review. As a result of this meticulous selection process, we obtained 20 articles for the review; Figure 1 describes our article selection process. This selection process allowed us to focus our review on the most valuable and relevant articles in the field of smart city security, ensuring that our review is based on the most pertinent literature. The final list of the selected articles is shown in Table 1.

A notable limitation of our review was the rigorous criteria which yielded only 20 articles. This choice was made among co-authors with the intention of maintaining a simplified narrative and exclusively focusing on research that met our selection criteria. While this strategy has the advantage of providing clarity, it also implies the exclusion of alternative or more nuanced perspectives, which yields clear disadvantages in comparison to other articles. It is important to note that these perspectives could be explored in future reviews, reflecting the constantly evolving nature of this field of study. Despite the shortcomings encountered during the conduct of this review, we have managed to acquire the essential information to carry out this work.

3. Thematic Overview

In this section, a detailed analysis of the findings extracted from the previously compiled literature is conducted. These results are organized into categories closely linked to the central theme of this review. The main objective of this approach is to provide a solid structure for a more in-depth discussion of the gathered information. The categorization not only facilitates a more precise analysis but also allows for an effective contextualization of the findings within the defined thematic framework.

3.1 Vulnerabilities in industries

Industries play a fundamental role in the progress of smart cities, serving as a primary source of sustainability for the production of goods and services that benefit

Table 1. The final list of articles used in this review, including information for title, journal, year of publication and citation.

Title	Journal	Year	Citation
Internet of Things for Smart Cities	IEEE Internet of Things Journal	2014	[3]
A Comprehensive Study of Security of Internet-of-Things	IEEE Transactions on Emerging Topics in Computing	2017	[5]
Deceptive Attack and Defense Game in Honeypot-Enabled Networks for the Internet of Things	IEEE Internet of Things Journal	2016	[6]
Smart home security: challenges, issues and solutions at different IoT layers	The Journal of Supercomputing	2021	[4]
An Accurate Security Game for Low-Resource IoT Devices	IEEE Transactions on Vehicular Technology	2017	[7]
Deep Abstraction and Weighted Feature Selection for Wi-Fi Impersonation Detection	IEEE Transactions on Information Forensics and Security	2018	[8]
Malware Propagation in Large-Scale Networks	IEEE Transactions on Knowledge and Data Engineering	2015	[9]
Security and Privacy in Smart Cities: Challenges and Opportunities	IEEE Access	2018	[1]
Security and Privacy of Smart Cities: A Survey, Research Issues and Challenges	IEEE Communications Surveys and Tutorials	2019	[10]
IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey	Sensors	2018	[11]
Security and Privacy in Smart City Applications and Services: Opportunities and Challenges	Cybersecurity and Secure Information Systems	2019	[12]
Internet-of-Things-Based Smart Cities: Recent Advances and Challenges	IEEE Communications Magazine	2017	[13]
The Need for Cybersecurity in Industrial Revolution and Smart Cities	Sensors	2022	[14]
An overview of security and privacy in smart cities' IoT communications	Transactions on Emerging Telecommunications Technologies	2019	[15]
Security for smart cities	IET Smart Cities	2020	[16]
Security and privacy challenges in smart cities	Sustainable Cities and Society	2018	[17]
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 and Security	2019	[18]
IoT-based smart homes: A review of system architecture, software, communications, privacy and security	Internet of Things	2018	[19]
Strategic Honeypot Game Model for Distributed Denial of Service Attacks in the Smart Grid	IEEE Transactions on Smart Grid	2017	[20]
Cyber security challenges in Smart Cities: Safety, security and privacy	Journal of Advanced Research	2014	[21]

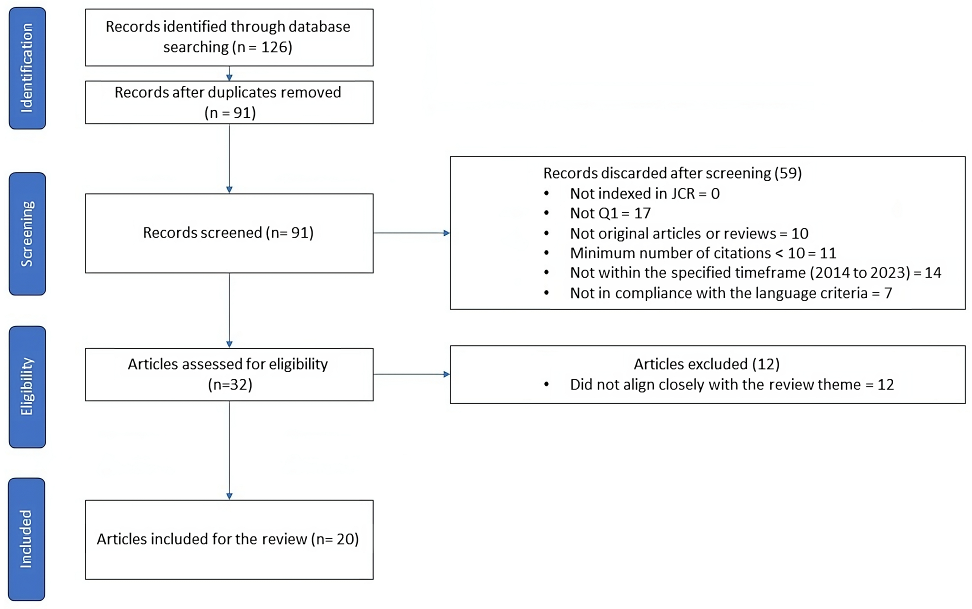
Identification
Records identified through database searching (n = 126)
Records after duplicates removed (n = 91)
Screening
Records screened (n= 91)
Records discarded after screening (59)
• Not indexed in JCR = 0
• Not Q1 = 17
• Not original articles or reviews = 10
• Minimum number of citations < 10 = 11
• Not within the specified timeframe (2014 to 2023) = 14
• Not in compliance with the language criteria = 7
Eligibility
Articles assessed for eligibility (n=32)
Articles excluded (12)
• Did not align closely with the review theme = 12
Included
Articles included for the review (n= 20)

Figure 1. The selection process flowchart, illustrating the systematic screening and selection methodology used to determine the final set of articles included in the review. Starting with 126 records identified through database searching, the process details the removal of duplicates, screening for relevance, assessment of eligibility based on predefined criteria, and the final inclusion of 20 articles that closely align with the review theme.

the population [22]. Globally, industries have undergone evolution and incorporated the use of technologies to drive their activities more efficiently and facilitate their development, logistics, and production [14]. However, in the industrial realm, issues related to security arise, directly impacting the smart urban fabric.

One of the initial vulnerabilities is found in companies that maintain outdated infrastructure, which hampers security due to limited maintenance of their systems. Another present vulnerability is associated with the use of inadequately tested software, creating a security gap for attackers, as this software is established with unauthenticated configurations [4]. Additionally, a vulnerability is observed in the implementation of data encryption protocols, a critical aspect for the security of employees and the general population, both in industries and urban areas. These protocols turn out to be weak, exposing employees' systems [14]. This situation exposes personal data and company credentials, potentially leading to identity theft or impersonation attacks [4], causing conflicts and losses in the industrial sector and significantly affecting the development of smart cities.

3.2 Vulnerability in smart homes

Smart cities are composed of smart businesses and homes that host the entire population within these urban areas. In the context of smart homes, these are defined as IoT-connected applications, where physical components are linked to the internet [4], creating an intelligent ecosystem that enhances the quality of life for inhabitants in a smart city. However, these ecosystems are not exempt from the issues present in cities.

Security is one of the main challenges in IoT due to the wireless medium and the information present in devices [7]. It is crucial to consider the IoT layers in smart homes to ensure certain protection against potential malicious attacks. These layers include the perception layer, where sensors collect and process information before sending it to the network layer. The network layer is responsible for communicating this information to connected devices, using wireless sensors like Wireless Sensor Networks (WSN) and the internet [15, 11]. This layer is bounded by the instructions of the application layer, which provides services for users to interact with their environment.

At application level, common security issues include phishing and malicious code, originating from user imprudence [9]. Another threat is Ransomware, representing data hijacking through the use of encryption to obtain a ransom from the user for their own data [19]. Additionally, the possibility of intentional attacks by third parties seeking to compromise wireless devices for malicious purposes, such as data theft through malware or hacking of these devices, cannot be ruled out. A potential solution to IoT vulnerabilities is the use of the Honeypot method, based on using a decoy to detect malicious intruders attempting to harm IoT networks comprising a smart home [6] and, in turn, the infrastructure of a smart city. However, this does not guarantee invulnerability, as it can be detected by Anti-Honeypot, used by cyber attackers. These layers are vulnerable to attacks, especially due to the poor management of IoT wireless devices.

3.3 Challenges for the smart cities

Smart cities aim to become environments designed to meet the basic needs of the population. It is estimated that by the year 2050, approximately 66% of the population will reside in urban environments [10], driven by significant population growth and migration from rural to metropolitan areas. This demographic shift entails a considerable increase in crime rates, especially concerning attacks and vulnerabilities targeted towards smart city infrastructure [16], particularly in the network that connects various urban areas.

For the proper functioning of smart cities, various layers with specific functions are implemented. The detection layer employs various tools to collect data from the environment, while the data collection layer stores the information obtained, both from network traffic and smart homes. The data processing layer manages the stored information, and the application and intelligent processing layer facilitates data exchange between citizens and relevant users such as stakeholders [13]. The harmony of these layers allows the proper functioning of smart cities.

However, when managing large volumes of data, these layered systems become vulnerable to third-party attacks, which may aim at stealing or misusing information. If an unauthorized user accesses this information, confidentiality is compromised, leading to what is known as an interception attack [12], which poses a problem in the flow of information in intelligent environments.

For a smart city to develop based on IoT, it is crucial to address certain aspects. This includes privacy-conscious communication, the implementation of efficient security preventive measures, and the conduct of a risk assessment to identify security gaps or threats [23]. This approach underscores the importance of considering these aspects to successfully create a smart city. In this context, the Chinese government establishes key criteria for technological and population development in its cities [18], highlighting fundamental points for a smart city to be genuinely viable. Among these, the need for a resilient infrastructure, a secure cyberspace, and the establishment of strong international partnerships are emphasized.

3.4 Threats for the smart cities

In addition to the challenges present in smart cities, there are also threats that significantly impact them, causing damage to both infrastructure and citizens privacy. Malware is malicious software created by attackers with the goal of compromising infrastructure and exploiting systems, often for financial and political reasons. This stands out as a major threat in this environment, representing a substantial challenge and security risk [9]. A clear example of this is the Botnet, a network of compromised computers controlled remotely by malware that carries out attacks on Domain Name Systems (DNS) and Internet Protocol (IP) addresses, thereby creating vulnerabilities in privacy.

Another common threat is phishing, which generates spam with the intent of collecting information through enticing ads for the user. Additionally, there are threats focused on the system of devices, such as Hardware-Trojans [5], which are modifications of integrated circuits allowing attackers to remotely access data or software. Malware also affects mobile devices through networks like Bluetooth or Wi-Fi [9], posing a threat to both citizens and infrastructure.

A primary threat in urban environments revolves around the vulnerability of location data through devices with Global Positioning System (GPS) [21], which can be intercepted by third parties, compromising detailed location-based information. This risk addresses general aspects of prevention, detection, and recovery from security compromises. A clear example of this issue is observed in the United States, where GPS surveillance poses a legal problem [17], as these devices can collect large volumes of user data, raising concerns about potential theft or attacks on databases that would impact privacy.

Biometrics, often underestimated, poses a significant risk in the context of smart cities. From fingerprints to retinas, facial data, and electronic signatures, these biometric data become a treasure for intruders. They provide access to sensitive information, such as banking status, facilitating the execution of fraud and threatening privacy by gaining access to user's personal accounts [1]. This information, increasingly common today, can be a key component in the infrastructure and vital data of the citizenry in an intelligent environment. Furthermore, it is crucial to consider the use of these elements to prevent the leakage of private data.

Smart cities face various vulnerabilities that impact both industries and smart homes. In industries, outdated infrastructure and the use of inadequately tested software create security gaps, exposing data and credentials to potential attacks [22], additionally, the implementation of weak protocols in data encryption adds significant risks. In the realm of smart homes, security is challenged by vulnerabilities in IoT layers [6], where poor management of wireless devices exposes to phishing, malicious code, and possible intentional attacks. Despite the benefits, these layers are prone to malicious attacks compromising the privacy of citizens.

The management of large volumes of data in specific layers also presents vulnerabilities, with threats to the confidentiality, authenticity, and integrity of information. Moreover, trojans pose a specific threat to the device system, affecting both mobile devices and other devices through networks like Bluetooth or Wi-Fi [8], with identity theft being a common attack. In the case of Wi-Fi, it is crucial to implement protective measures since it is essential for communication among various IoT devices. Wi-Fi security thus becomes one of the key considerations in this intelligent environment; to safeguard it, the use of control protocols like Mandatory Access Control (MAC) or the Wi-Fi Protected Access (WPA) protocol is necessary [16], providing more sophisticated data encryption.

Furthermore, the vulnerability of location data through GPS devices also stands out as a significant threat in this context. When comparing security factors and the approach to a smart city, there are many deficiencies regarding privacy and technological infrastructure [21], this poses multiple challenges to consider for potential threats that could jeopardize a general population, implying a restructuring of the plan for a smart city, taking into account the points raised in the theme of this review.

4. Discussion

When exploring vulnerabilities in industries within the context of smart cities, a complex network of challenges threatening urban sustainability and efficiency is revealed [24], posing a significant challenge for this environment.

In smart cities, security is challenged by crucial threats that compromise the infrastructure, data, and privacy of inhabitants. Both traditional crime and digital threats impact major industries, creating vulnerabilities in software due to inadequate maintenance. Furthermore, smart homes exhibit deficiencies in IoT device security [7, 9], exposing them to risks such as phishing and potential hacking.

Additionally, highlighted are additional dangers, such as the unauthorized use of biometrics, introducing significant risks [25], including banking fraud through the misuse of biometric data. This discovery not only resonates with the warnings from existing literature regarding the risks associated with outdated technology but also underscores the urgency for new cybersecurity research in the era of industrial digitization [20, 15]. Furthermore, vulnerabilities associated with the use of untested software and weak encryption protocols highlight the need to strengthen computer security. These findings not only broaden our understanding of current challenges but also align with the prevailing narrative, emphasizing the need for comprehensive approaches to bolster infrastructure in smart cities.

These issues highlight the vulnerability of these interconnected ecosystems, emphasizing the importance of user awareness and preventive measures. Our review not only provides a detailed insight into specific vulnerabilities but also seamlessly integrates into the overarching narrative of security in smart cities, underscoring the critical need for preventive measures in the layers of urban data processing.

This review, we believe, has implications in recognizing contemporary vulnerabilities and threats for smart cities. Examining vulnerabilities in both industries and smart home environments highlights the necessity of adopting more secure approaches to strengthen these areas in response to identified threats. The aforementioned findings support the importance of updates and maintenance in industrial infrastructures, along with the implementation of robust security protocols and strategies [26, 20], such as user awareness and preventive measures, including the use of Honeypots to enhance threat detection in smart environments. These results contribute to advance knowledge in the field of urban cybersecurity and to provide diverse strategies and solutions for the development of policies and practices that reinforce security in smart urban environments [1]. This plays a crucial role in the planning of a smart city by considering potential risks and vulnerabilities.

According to our findings, security is essential for all IoT devices. As smart cities provide internet connectivity to a wide variety of devices, security becomes a highly critical challenge. These findings are reinforced by analyzing previous research on the subject, as around 70% of IoT devices in a smart city were at risk of attacks [13]; this vulnerability stemmed from the inadequate software security and vulnerabilities in encryption within communication protocols.

It is important to acknowledge that our review may be affected by some bias stemming from the timing of the publication of the collected articles. This could lead to discrepancies between our interpretations and those obtained by other research, which, in turn, could contribute to potential errors in our analysis.

Furthermore, during the development of this work, we encountered several limitations that complicated the development process. Among them, the quantity of articles available for review, and the publication dates of some articles stand out. Additionally, we identified certain information gaps that our review could not fully address. For example, we could not include specific strategies applied to protect data in smart environments, as we focused exclusively on identifying threats and vulnerabilities present in smart cities. This limitation creates a gap in our review that could be the subject of future research: improving information organization and data collection, considering the search scope to obtain relevant and updated information.

Furthermore, our review has pinpointed literature gaps that deserve exploration in future research. We highlight some outstanding thematic areas: What could be viable solutions in the context of a smart city? What regulations could be adopted by governments to prevent risks in smart cities? How have technical challenges in cybersecurity in smart urban environments been addressed? What threats and solutions have emerged in the realm of smart vehicles? What are the most prominent threats to the development of smart cities? These questions represent valuable opportunities for future research.

In smart cities, security faces threats that compromise infrastructure and data, generating vulnerabilities [27, 15]; hence, efficient strategies are necessary to address these challenges. The review highlights complex challenges in smart industries and homes, ranging from outdated infrastructures to weak encryption protocols. This implies adopting secure approaches and user awareness strategies to strengthen security [28]. These findings contribute to the knowledge in urban cybersecurity, enabling the development of security policies in smart cities. Furthermore, the need for future research is emphasized to address identified gaps and enhance understanding of security in intelligent urban environments.

5. Conclusion

During the elaboration of this article, we have compiled the most relevant and up-to-date research in the cybersecurity field, following our selection criteria. Subsequently, we conducted a literature analysis, allowing us to categorize the themes addressed in the articles to achieve a deeper understanding of the information. This process led to the discussion, where the previously exposed themes were thoroughly addressed, seeking a satisfactory consensus on the analyzed information. Finally, we will present our conclusions derived from the analysis and interpretation of the themes.

Our article highlights vulnerabilities in industries and smart homes, as well as challenges and threats for smart cities in general. In industries, the issue of outdated infrastructure, inadequately tested software, and weaknesses in encryption protocols [4] stands out, exposing data and credentials to potential attacks. In smart homes, IoT security is crucial, with layers vulnerable to attacks such as phishing and malicious code [6]. Additionally, demographic and criminal challenges in smart cities are prominent, along with the need to address data management security. Threats include malware, botnets, phishing, and the vulnerability of location data through GPS, as well as the risk of biometrics to citizens privacy. The most significant risk associated with citizens is information theft through data detection layer attacks [13, 12]; this could lead to a case of ransomware or identity theft, directly jeopardizing the security of the citizens.

It is expected that this article will emphasize security aspects in smart cities, considering significant issues such as privacy, infrastructure, and industry vulnerabilities, to develop a smart environment adequately, assuming citizen participation, and addressing the significant challenges of smart urbanization. Likewise, this review is estimated to emphasize future research covering observed gaps, favor future research with relevant information, and significantly contribute to an overall understanding of security and potential study objects contributing to new findings and advances in the field of cybersecurity for urban environments.

This review highlights various limitations in previous sections. One of the most prominent is the restriction on the number of citations per year in articles excludes those that could provide valuable or more updated information on the topics addressed in this article. Another limiting aspect was the absence of a central focus on possible solutions to threats and vulnerabilities in intelligent environments. Instead, we focused exclusively on addressing contemporary challenges related to vulnerabilities and threats impacting smart cities. All these limitations are essential elements to consider for future reviews, contributing to strengthening the identified weaknesses in this review.

Given the limitations that we have identified, gaps and openings have been revealed that offer opportunities for future research and valuable contributions to the study field. An example is the need to more comprehensively address possible solutions to the issues mentioned in this review, as well as delve into how cybersecurity challenges have been faced, especially in specific areas of smart city development. On the other hand, the emergence of new, more sophisticated threats could present an opportunity for further research. As can be seen, there are various areas of research to explore, with a crucial focus on security in the context of smart cities.

During the review, we have explored the current landscape of threats and vulnerabilities in network security in the context of smart cities. By identifying and analyzing the challenges and gaps in existing research, we have compiled detailed complexities and vulnerabilities inherent in this technological environment. Smart cities are a fascinating field full of potential, but they also present significant challenges that require a lot of attention. Our work not only highlights these critical issues but also describes possible directions for future research, paving the way for future research that will change the way we think and protect smart cities.

References

[1] L. Cui, G. Xie, Y. Qu, L. Gao, and Y. Yang, “Security and Privacy in Smart Cities: Challenges and Opportunities,” *IEEE Access*, vol. 6, pp. 46 134–46 145, 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8409952/

[2] S. Srivastava, A. Bisht, and N. Narayan, “Safety and security in smart cities using artificial intelligence — A review,” in *2017 7th International Conference on Cloud Computing, Data Science Engineering - Confluence*, vol. 6. IEEE, jan 2017, pp. 130–133. [Online]. Available: http://ieeexplore.ieee.org/document/7943136/

[3] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, “Internet of Things for Smart Cities,” *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22–32, feb 2014. [Online]. Available: https://ieeexplore.ieee.org/document/6740844/

[4] H. Touqeer, S. Zaman, R. Amin, M. Hussain, F. Al-Turjman, and M. Bilal, *Smart home security: challenges, issues and solutions at different IoT layers.* Springer US, 2021, vol. 77, no. 12. [Online]. Available: https://doi.org/10.1007/s11227-021-03825-1

[5] A. Mosenia and N. K. Jha, "A Comprehensive Study of Security of Internet-of-Things," *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 4, pp. 586–602, oct 2017. [Online]. Available: http://ieeexplore.ieee.org/document/7562568/

[6] Q. D. La, T. Q. S. Quek, J. Lee, S. Jin, and H. Zhu, "Deceptive Attack and Defense Game in Honeypot-Enabled Networks for the Internet of Things," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 1025–1035, dec 2016. [Online]. Available: http://ieeexplore.ieee.org/document/7442780/

[7] H. Sedjelmaci, S. M. Senouci, and T. Taleb, "An Accurate Security Game for Low-Resource IoT Devices," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 10, pp. 9381–9393, oct 2017. [Online]. Available: http://ieeexplore.ieee.org/document/7920414/

[8] M. E. Aminanto, R. Choi, H. C. Tanuwidjaja, P. D. Yoo, and K. Kim, "Deep Abstraction and Weighted Feature Selection for Wi-Fi Impersonation Detection," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 3, pp. 621–636, mar 2018. [Online]. Available: http://ieeexplore.ieee.org/document/8067440/

[9] S. Yu, G. Gu, A. Barnawi, S. Guo, and I. Stojmenovic, "Malware Propagation in Large-Scale Networks," *IEEE Transactions on Knowledge and Data Engineering*, vol. 27, no. 1, pp. 170–179, jan 2015. [Online]. Available: https://ieeexplore.ieee.org/document/6807753/

[10] M. Sookhak, H. Tang, Y. He, and F. R. Yu, "Security and Privacy of Smart Cities: A Survey, Research Issues and Challenges," *IEEE Communications Surveys Tutorials*, vol. 21, no. 2, pp. 1718–1743, 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8447209/

[11] M. Burhan, R. Rehman, B. Khan, and B.-S. Kim, "IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey," *Sensors*, vol. 18, no. 9, p. 2796, aug 2018. [Online]. Available: http://www.mdpi.com/1424-8220/18/9/2796

[12] A. Verma, A. Khanna, A. Agrawal, A. Darwish, and A. E. Hassanien, "Security and Privacy in Smart City Applications and Services: Opportunities and Challenges," in *Advanced Sciences and Technologies for Security Applications.* Springer International Publishing, 2019, pp. 1–15. [Online]. Available: http://link.springer.com/10.1007/978-3-030-16837-7_1

[13] Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran, and S. Guizani, "Internet-of-Things-Based Smart Cities: Recent Advances and Challenges," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 16–24, 2017. [Online]. Available: http://ieeexplore.ieee.org/document/8030479/

[14] A. Clim, A. Toma, R. D. Zota, and R. Constantinescu, "The Need for Cybersecurity in Industrial Revolution and Smart Cities," *Sensors*, vol. 23, no. 1, p. 120, dec 2022. [Online]. Available: https://www.mdpi.com/1424-8220/23/1/120

[15] F. Al-Turjman, H. Zahmatkesh, and R. Shahroze, "An overview of security and privacy in smart cities' IoT communications," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 3, pp. 1–19, mar 2019. [Online]. Available: https://onlinelibrary.wiley.com/doi/10.1002/ett.3677

[16] C. K. Toh, "Security for smart cities," *IET Smart Cities*, vol. 2, no. 2, pp. 95–104, jul 2020. [Online]. Available: https://onlinelibrary.wiley.com/doi/10.1049/iet-smc.2020.0001

[17] T. Braun, B. C. Fung, F. Iqbal, and B. Shah, "Security and privacy challenges in smart cities," *Sustainable Cities and Society*, vol. 39, pp. 499–507, may 2018. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S2210670717310272

[18] M. Vitunskaite, Y. He, T. Brandstetter, and H. Janicke, "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 and Security*, vol. 83, pp. 313–331, 2019. [Online]. Available: https://doi.org/10.1016/j.cose.2019.02.009

[19] D. Mocrii, Y. Chen, and P. Musilek, "IoT-based smart homes: A review of system architecture, software, communications, privacy and security," *Internet of Things*, vol. 1-2, pp. 81–98, sep 2018. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S2542660518300477

[20] K. Wang, M. Du, S. Maharjan, and Y. Sun, "Strategic Honeypot Game Model for Distributed Denial of Service Attacks in the Smart Grid," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2474–2482, sep 2017. [Online]. Available: http://ieeexplore.ieee.org/document/7857804/

[21] A. S. Elmaghraby and M. M. Losavio, "Cyber security challenges in smart cities: Safety, security and privacy," *Journal of Advanced Research*, vol. 5, no. 4, pp. 491–497, 2014. [Online]. Available: http://dx.doi.org/10.1016/j.jare.2014.02.006

[22] L. Fang, H. Zhang, M. Li, C. Ge, L. Liu, and Z. Liu, "A Secure and Fine-Grained Scheme for Data Security in Industrial IoT Platforms for Smart City," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 7982–7990, sep 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9104725/

[23] Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran, and S. Guizani, "Internet-of-Things-Based Smart Cities: Recent Advances and Challenges," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 16–24, 2017. [Online]. Available: http://ieeexplore.ieee.org/document/8030479/

[24] S. Alromaihi, W. Elmedany, and C. Balakrishna, "Cyber Security Challenges of Deploying IoT in Smart Cities for Healthcare Applications," in *2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*. IEEE, aug 2018, pp. 140–145. [Online]. Available: https://ieeexplore.ieee.org/document/8488188/

[25] A. Ross, S. Banerjee, and A. Chowdhury, "Security in smart cities: A brief review of digital forensic schemes for biometric data," *Pattern Recognition Letters*, vol. 138, pp. 346–354, oct 2020. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0167865520302555

[26] Feng Zhang, Shijie Zhou, Zhiguang Qin, and Jinde Liu, "Honeypot: a supplemented active defense system for network security," in *Proceedings of the 8th International Scientific and Practical Conference of Students, Post-graduates and Young Scientists. Modern Technique and Technologies. MTT'2002 (Cat. No.02EX550)*. IEEE, 2003, pp. 231–235. [Online]. Available: http://ieeexplore.ieee.org/document/1236295/

[27] T. H. Vo, W. Fuhrmann, K.-P. Fischer-Hellmann, and S. Furnell, "Identity-as-a-Service: An Adaptive Security Infrastructure and Privacy-Preserving User Identity for the Cloud Environment," *Future Internet*, vol. 11, no. 5, p. 116, may 2019. [Online]. Available: https://www.mdpi.com/1999-5903/11/5/116

[28] K. A. Alissa, B. AlDeeb, H. A. Alshehri, S. A. Dahdouh, B. M. Alsubaie, A. M. Alghamdi, and M. Alsmadi, "Developing a simulated intelligent instrument to measure user behavior toward cybersecurity policies," *International Journal of Communication Networks and Information Security (IJCNIS)*, vol. 13, no. 1, pp. 82–91, apr 2022. [Online]. Available: https://www.ijcnis.org/index.php/ijcnis/article/view/4923