Open Access Research Journal of
Multidisciplinary Studies
Journals home page: https://oarjpublication/journals/oarjms/
ISSN: 2783-0268 (Online)

OARJ OPEN ACCESS RESEARCH JOURNALS

(Review Article)

Securing the smart city: A review of cybersecurity challenges and strategies

Johnson Sunday Oliha [1, *], Preye Winston Biu [2] and Ogagua Chimezie Obi [1]

[1] *Independent Researcher, Lagos, Nigeria.*
[2] *INEC Nigeria.*

Open Access Research Journal of Multidisciplinary Studies, 2024, 07(01), 094–101

Publication history: Received on 31 December 2023; revised on 08 February 2024; accepted on 10 February 2024

Article DOI: https://doi.org/10.53022/oarjms.2024.7.1.0013

Abstract

In the era of rapid urbanization and technological advancement, the emergence of smart cities promises innovative solutions to urban challenges. However, the integration of various technologies into urban infrastructures also exposes cities to unprecedented cybersecurity threats. This review presents a comprehensive review of the cybersecurity challenges faced by smart cities and explores the strategies to mitigate these risks. Smart cities leverage interconnected networks of sensors, devices, and systems to enhance efficiency, sustainability, and citizen services. Yet, this interconnectedness creates a complex attack surface vulnerable to cyber threats. One of the primary challenges is the diverse range of IoT devices deployed across smart city infrastructures, often lacking robust security mechanisms. These devices are susceptible to exploitation by cybercriminals for malicious activities, such as data breaches, sabotage, and surveillance. Moreover, the interconnected nature of smart city systems amplifies the potential impact of cyberattacks, posing significant risks to critical infrastructure, public safety, and privacy. Threat actors can exploit vulnerabilities in interconnected systems to disrupt essential services, manipulate data, or even cause physical harm. As smart cities rely on data-driven decision-making, the integrity and confidentiality of data become paramount concerns. To address these challenges, various cybersecurity strategies have been proposed and implemented. These strategies encompass a multi-layered approach, integrating technical solutions, regulatory frameworks, and collaboration among stakeholders. Technical measures include encryption, authentication mechanisms, intrusion detection systems, and secure software development practices. Additionally, implementing robust access controls and network segmentation can limit the scope of potential attacks. Furthermore, regulatory initiatives play a crucial role in enhancing cybersecurity standards and promoting compliance among smart city stakeholders. Establishing clear guidelines for data protection, privacy rights, and incident response protocols is essential to safeguarding citizens' interests. Collaboration among government agencies, private sector partners, academia, and cybersecurity experts fosters information sharing and collective defense against emerging threats. Securing smart cities against cybersecurity threats requires a concerted effort to address the multifaceted challenges posed by interconnected technologies. By implementing comprehensive strategies encompassing technical measures, regulatory frameworks, and collaborative approaches, smart cities can mitigate risks and foster a resilient and secure urban environment for all citizens.

Keywords: Smart City; Cybersecurity; AI; Technology; Security; Review

1. Introduction

In the wake of rapid urbanization and technological advancement, the concept of smart cities has emerged as a promising solution to address the complex challenges of modern urban environments. Smart cities integrate various Information and Communication Technologies (ICT) and Internet of Things (IoT) devices to enhance the efficiency, sustainability, and quality of life for residents. These interconnected systems enable cities to optimize resource allocation, improve public services, and promote economic growth.

* Corresponding author: Johnson Sunday Oliha

Smart cities leverage digital technologies to gather data from sensors, devices, and infrastructure, which is then analyzed to gain insights and facilitate informed decision-making. This data-driven approach enables cities to efficiently manage resources, reduce environmental impact, and enhance overall urban livability (Alfouzan, 2022). The implementation of smart city technologies offers numerous benefits, including improved infrastructure efficiency, enhanced public services, and greater economic competitiveness (Zhao & Zhang, 2020). For example, smart transportation systems can reduce traffic congestion and carbon emissions, while smart energy grids enable more sustainable energy consumption patterns (Zhao & Zhang, 2020).

However, along with these benefits come significant challenges. Challenges of smart city technologies include the complexity of integrating diverse systems and technologies, ensuring interoperability and scalability, addressing privacy concerns related to data collection and usage, and managing cybersecurity risks (Clim et al., 2022). As smart cities become increasingly reliant on digital infrastructure and interconnected systems, cybersecurity emerges as a critical consideration in their development and operation (Kim et al., 2023). The integration of IoT devices, sensors, and networks in smart cities creates a vast attack surface that is susceptible to cyber threats (Raimundo & Rosário, 2022). Cyberattacks targeting smart city infrastructures can have severe consequences, including disruption of essential services, compromise of sensitive data, and threats to public safety (Kim et al., 2023). Therefore, ensuring the cybersecurity of smart city systems is paramount to safeguarding the integrity, availability, and confidentiality of critical infrastructure and citizen information (Ahmadi-Assalemi et al., 2020).

In addressing the cybersecurity challenges, it is essential to consider the specific threats associated with data exchange in smart cities and their potential consequences (Clim et al., 2022). Additionally, a comprehensive understanding of the smart city threat landscape, challenges related to data acquisition and storage, and the importance of cyber resilience and incident response is crucial (Alfouzan, 2022; Ahmadi-Assalemi et al., 2020). Furthermore, the interconnectedness of intelligent devices and the major concerns in smart cities related to cybersecurity, including communication infrastructures, cloud computing, smart health, and energy management, need to be carefully addressed (Raimundo & Rosário, 2022). It is also important to conduct thorough cybersecurity risk assessments in smart city infrastructures to identify and mitigate potential threats, especially those aimed at breaching privacy and security (Kalinin et al., 2021).

While smart cities offer numerous benefits, they also present significant cybersecurity challenges that must be effectively addressed to ensure the integrity, availability, and confidentiality of critical infrastructure and citizen information. This requires a comprehensive understanding of the smart city threat landscape, proactive cyber resilience and incident response strategies, and thorough cybersecurity risk assessments to mitigate potential threats.

In this context, this paper reviews the cybersecurity challenges faced by smart cities and explores strategies to mitigate these risks. By addressing the complex cybersecurity landscape of smart cities, stakeholders can foster a resilient and secure urban environment that leverages the benefits of digital innovation while mitigating associated risks.

2. Cybersecurity Challenges in Smart Cities

Smart cities, heralded as the epitome of urban innovation, are not immune to the myriad cybersecurity challenges that accompany their technological advancements. The integration of diverse Information and Communication Technologies (ICT) and Internet of Things (IoT) devices within urban infrastructure presents a complex cybersecurity landscape fraught with vulnerabilities and risks. This section delves into the multifaceted cybersecurity challenges faced by smart cities, ranging from the diversity and complexity of IoT devices to the evolving threat landscape.

The cybersecurity challenges in smart cities are multifaceted and stem from various factors such as the proliferation of IoT devices with inconsistent security measures, legacy systems with inadequate security features, and the interconnected nature of smart city systems (Argaw et al., 2020; Radoglou-Grammatikis et al., 2021; Auffret et al., 2017). IoT devices often lack standardized security protocols, making them susceptible to exploitation by malicious actors, and legacy systems may lack built-in security features or receive infrequent updates and patches, rendering them vulnerable to exploitation (Argaw et al., 2020; Radoglou-Grammatikis et al., 2021). The interconnected nature of smart city systems significantly expands the attack surface, providing adversaries with numerous entry points to exploit, and compromising a single component can have far-reaching implications, leading to cascading cyberattacks across multiple systems (Radoglou-Grammatikis et al., 2021; Auffret et al., 2017). Furthermore, the collection and storage of sensitive information in smart cities pose significant data security and privacy concerns, making them an attractive target for cybercriminals seeking to exploit or monetize this information (Argaw et al., 2020; Algarni et al., 2021).

Smart cities face a diverse range of cyber threats, including malware infections, ransomware attacks, distributed denial-of-service (DDoS) attacks, and insider threats, which can target critical infrastructure components, IoT devices, communication networks, and data repositories, posing significant risks to the operation and integrity of smart city systems (Radoglou-Grammatikis et al., 2021; Auffret et al., 2017). Recent high-profile cyberattacks targeting smart cities worldwide, such as the ransomware attack on the city of Atlanta in 2018 and the 2020 cyberattack on the city of New Orleans, underscore the severity and real-world impact of cyber threats on smart city infrastructures (Fabian et al., 2023; Radoglou-Grammatikis et al., 2021; Auffret et al., 2017).

The cybersecurity challenges in smart cities are complex and require comprehensive strategies to address the vulnerabilities associated with IoT devices, legacy systems, interconnected networks, and data security. Mitigating these risks necessitates a holistic approach that encompasses standardized security protocols for IoT devices, robust security features for legacy systems, and effective measures to protect sensitive data from cyber threats.

In conclusion, cybersecurity challenges pose significant risks to the resilience, integrity, and security of smart cities. Addressing these challenges requires a concerted effort from city authorities, technology vendors, cybersecurity experts, and other stakeholders to implement robust security measures, enhance threat detection capabilities, and foster a culture of cybersecurity awareness and resilience. By proactively addressing cybersecurity challenges, smart cities can mitigate risks, protect critical infrastructure, and ensure the safety and well-being of their residents.

3. Strategies for Cybersecurity in Smart Cities

Smart cities, with their interconnected systems and reliance on digital technologies, require robust cybersecurity strategies to mitigate risks and safeguard critical infrastructure and citizen data. This section outlines key strategies for enhancing cybersecurity in smart cities, ranging from technical measures to regulatory frameworks and collaboration initiatives. Implementing strong encryption protocols ensures that data transmitted between IoT devices, sensors, and central systems remains secure and confidential. Encryption protects sensitive information from unauthorized access and interception by encrypting data in transit and at rest.

Deploying robust authentication mechanisms, such as multi-factor authentication (MFA) and digital certificates, is crucial for verifying the identity of users and devices accessing smart city systems (Uchechukwu et al., 2023; Nguyen et al., 2019). Authentication ensures that only authorized individuals or devices can access sensitive data and resources, mitigating the risk of unauthorized access and insider threats. Additionally, implementing Role-Based Access Control (RBAC) enables smart city administrators to define and enforce granular access permissions based on users' roles and responsibilities, minimizing the risk of privilege escalation and unauthorized access (Aldribi & Singh, 2022).

Furthermore, IDPS solutions continuously monitor smart city networks and systems for suspicious activity and potential security breaches (Pieroni et al., 2018). These systems employ advanced analytics and machine learning algorithms to detect anomalous behavior and respond to security incidents in real-time, minimizing the impact of cyber threats. Moreover, segmenting smart city networks based on sensitivity levels and functional requirements helps contain the impact of security breaches and limit lateral movement by attackers (Wang et al., 2018; Adeleke et al., 2019). By isolating critical infrastructure components and sensitive data repositories, network segmentation reduces the attack surface and enhances overall security posture.

Adhering to secure software development practices, such as incorporating security requirements into the software development lifecycle (SDLC) and conducting regular code reviews and vulnerability assessments, helps mitigate vulnerabilities and reduce the risk of introducing security flaws into smart city applications and services (Dash & Sharma, 2022). Enacting cybersecurity legislation and regulations specific to smart city environments establishes legal requirements and standards for cybersecurity practices and risk management, fostering accountability and transparency in cybersecurity governance (Schaffers et al., 2011). Compliance with data protection and privacy regulations, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), helps safeguard citizen privacy rights and protect personal data collected and processed by smart city systems (Li et al., 2019; Ilugbusi et al., 2020).

Collaborative partnerships between government agencies, technology vendors, academia, and cybersecurity experts facilitate knowledge sharing, resource pooling, and collective action against cyber threats (Gotlib et al., 2020; Vincent et al., 2021). By fostering collaboration, smart cities can leverage the expertise and resources of diverse stakeholders to strengthen cybersecurity defenses and resilience. Establishing mechanisms for sharing threat intelligence and best practices enables smart city stakeholders to stay informed about emerging cyber threats and effective mitigation strategies (Mitton et al., 2012; Abrahams et al., 2023). By sharing information on cyber threats, vulnerabilities, and incident response strategies, stakeholders can proactively identify and address cybersecurity risks, enhancing the overall security posture of smart cities.

In conclusion, adopting comprehensive cybersecurity strategies is imperative for ensuring the resilience and security of smart cities in the face of evolving cyber threats. By implementing technical measures, access controls, regulatory frameworks, and collaboration initiatives, smart cities can mitigate risks, protect critical infrastructure, and safeguard citizen data, thereby fostering trust and confidence in the digital transformation of urban environments.

4. Case Studies and Examples

Singapore has been widely recognized for its proactive approach to cybersecurity in the context of smart city development. The city-state has established the Cyber Security Agency (CSA), which collaborates with government agencies, private sector partners, and academia to develop robust cybersecurity strategies and initiatives (Pollini et al., 2021). Singapore's National Cybersecurity Strategy emphasizes the importance of public-private partnerships, information sharing, and capacity building to enhance cybersecurity resilience (Pollini et al., 2021). Additionally, Singapore has implemented advanced security measures, such as network segmentation, encryption, and continuous monitoring, to protect critical infrastructure and citizen data from cyber threats (Pollini et al., 2021).

Barcelona has also implemented innovative cybersecurity measures to protect its smart city infrastructure and services. The city's Barcelona Cybersecurity Centre (BCC) serves as a centralized hub for monitoring and responding to cyber threats targeting smart city systems (Deibert, 2018). Barcelona has also invested in cybersecurity awareness campaigns and training programs to educate citizens and employees about cybersecurity best practices and risks (Deibert, 2018). Furthermore, Barcelona has embraced open data initiatives while implementing stringent data protection measures to ensure the privacy and security of citizen data collected by smart city applications (Deibert, 2018).

The city of Atlanta experienced a ransomware attack in 2018 that disrupted essential services, costing the city millions of dollars in recovery efforts. The incident highlighted the importance of maintaining up-to-date security measures, conducting regular backups of critical data, and developing robust incident response plans to mitigate the impact of cyberattacks on smart city infrastructures. Tel Aviv has adopted an innovative approach to cybersecurity by leveraging artificial intelligence (AI) and machine learning algorithms to detect and respond to cyber threats in real-time. The city's Cyber Tel Aviv initiative collaborates with leading technology companies and startups to develop AI-powered cybersecurity solutions tailored to the unique challenges of smart cities. These AI-driven technologies enable proactive threat detection, rapid incident response, and adaptive security measures to safeguard smart city infrastructures and services. Helsinki has implemented a data-centric approach to cybersecurity in its smart city initiatives, prioritizing the protection of citizen data and privacy rights. The city's MyData initiative empowers citizens to control and manage their personal data, ensuring transparency and accountability in data handling practices (Hämäläinen, 2019). This innovative data governance model emphasizes the ethical and responsible use of data in smart city applications (Habibzadeh et al., 2019). Successful implementations of cybersecurity strategies in smart cities require a combination of technical measures, regulatory frameworks, and collaborative initiatives (Clim et al., 2022). By learning from past cyber incidents, adopting innovative approaches, and prioritizing the protection of citizen data and privacy rights, smart cities can enhance cybersecurity resilience and safeguard critical infrastructure against evolving cyber threats (Deibert, 2018).

The literature emphasizes the importance of a human-centric approach to cybersecurity, which involves aligning security needs with the removal of vulnerabilities (Cavelty, 2014). It is crucial to consider the role of civil society in implementing cybersecurity norms, as well as the need for usable transparency for dynamic risk assessment (Kumar, 2021; Collen et al., 2022). Furthermore, the value of criminological theories in explaining cybersecurity in smart cities is highlighted, emphasizing the practical implications for cybersecurity risks and potential hacking incidents (Cornelius et al., 2022).

In the context of smart cities, the use of IoT communications and blockchain for cybersecurity, as well as the application of deep learning techniques, is essential for assessing and mitigating cybersecurity risks (Al-Turjman et al., 2019; Andrade et al., 2020; Latif et al., 2021). Additionally, the need for cybersecurity in smart city infrastructures, such as smart grids, is underscored, with a focus on investigating cyber-attack methods and measures (Kalinin et al., 2021; Avci, 2021). The role of augmented reality and cybersecurity in smart cities is also highlighted, emphasizing the importance of strengthening policies related to cybersecurity (Alfouzan, 2022).

In conclusion, Helsinki's data-centric approach to cybersecurity in smart city initiatives, along with the adoption of innovative strategies and the consideration of human-centric cybersecurity, reflects a comprehensive and proactive stance towards safeguarding citizen data and privacy rights in the evolving landscape of cyber threats.

5. Future Directions and Emerging Trends

As smart cities continue to evolve and embrace digital technologies, cybersecurity threats and risks are also evolving, presenting new challenges for urban environments. Some emerging cybersecurity threats and risks include; With the increasing sophistication of cybercriminals and nation-state actors, smart cities face the risk of highly targeted and coordinated cyber attacks aimed at disrupting critical infrastructure, stealing sensitive data, or causing widespread chaos.

To address the increasing cybersecurity risks in smart cities, it is crucial to consider the proliferation of Internet of Things (IoT) devices, insider threats, and vulnerabilities in the supply chain of hardware and software components (Jannat et al., 2020; Ismagilova et al., 2020). The use of AI and machine learning algorithms, blockchain technology, quantum-safe cryptographic algorithms, and zero trust architecture are emerging trends and advancements in cybersecurity technologies tailored for smart cities (Shah et al., 2019; Li, 2020; Nikitas et al., 2020; Khan et al., 2019). Additionally, regulatory developments and policy initiatives, such as stricter data protection and privacy regulations, cybersecurity standards and certification programs, international collaboration, and public-private partnerships, are likely to shape the future of cybersecurity in smart cities (Neupane et al., 2021; Alhalafi & Veeraraghavan, 2021).

The literature emphasizes the importance of addressing privacy and security challenges in smart cities, particularly in the context of IoT and big data analytics technologies (Shah et al., 2019; Ismagilova et al., 2020). Furthermore, the trustworthiness of new technologies and the adoption of smart city technologies are considered important factors in addressing cybersecurity risks (Neupane et al., 2021; Cole & Tran, 2022). The development of smart city architecture frameworks and enterprise architecture development methodologies also plays a significant role in enhancing cybersecurity in smart cities (Prasetyo & Lubis, 2020; Prasetyo & Habibie, 2022). The evolving cybersecurity landscape in smart cities necessitates a comprehensive approach that encompasses technological advancements, regulatory frameworks, and trust-building measures to mitigate the risks associated with IoT proliferation, insider threats, and supply chain vulnerabilities (Mouchou et al., 2021).

In conclusion, future directions and emerging trends in cybersecurity for smart cities encompass evolving threats and risks, advancements in cybersecurity technologies, and potential regulatory developments and policy initiatives aimed at enhancing cybersecurity resilience and protecting citizen data and privacy rights in the digital urban landscape. By staying abreast of these trends and taking proactive measures, smart cities can navigate the evolving cybersecurity landscape and build secure and resilient urban environments for their residents

6. Recommendation and Conclusion

Smart cities face a myriad of cybersecurity challenges stemming from the complexity and interconnectedness of digital infrastructure, the proliferation of IoT devices, and the evolving threat landscape. These challenges include the diversity and vulnerabilities of IoT devices, the interconnectedness of smart city systems increasing the attack surface, data security and privacy concerns, and the evolving nature of cyber threats targeting critical infrastructure and citizen data.

Given the critical role of digital technologies in enhancing urban efficiency and sustainability, adopting comprehensive cybersecurity strategies is paramount for smart cities. A proactive approach to cybersecurity not only mitigates risks and safeguards critical infrastructure but also fosters trust and confidence among residents and stakeholders. By prioritizing cybersecurity, smart cities can protect citizen data, ensure the continuity of essential services, and mitigate the potentially devastating impacts of cyberattacks on urban environments. Stakeholders in smart city development, including government agencies, technology vendors, cybersecurity experts, and citizens, must prioritize cybersecurity as a fundamental aspect of urban planning and governance.

Foster collaboration and information sharing among government agencies, private sector partners, academia, and cybersecurity experts to develop and implement robust cybersecurity strategies tailored to smart city environments. Allocate resources and invest in cybersecurity capabilities, including technology, personnel, and training, to enhance threat detection, incident response, and resilience in smart city infrastructures. Ensure compliance with data protection and privacy regulations, cybersecurity standards, and best practices to safeguard citizen data and privacy rights in smart city initiatives. Educate citizens and employees about cybersecurity risks, best practices, and the importance of cybersecurity in smart city development through awareness campaigns, training programs, and community outreach initiatives. Continuously evaluate and improve cybersecurity measures, technologies, and policies to adapt to evolving cyber threats and ensure the resilience and security of smart city infrastructures.

In conclusion, addressing cybersecurity challenges in smart cities requires a concerted effort from all stakeholders to prioritize cybersecurity, adopt comprehensive strategies, and foster a culture of cyber resilience. By working together, smart cities can harness the benefits of digital innovation while effectively managing cybersecurity risks and ensuring the safety, security, and prosperity of urban communities.

Compliance with ethical standards

Disclosure of conflict of interest

The author has no conflict of interest in this research.

References

[1] Abrahams, T.O., Ewuga, S.K., Kaggwa, S., Uwaoma, P.U., Hassan, A.O. and Dawodu, S.O., 2023. Review of strategic alignment: Accounting and cybersecurity for data confidentiality and financial security.

[2] Adeleke, O.K., Segun, I.B. and Olaoye, A.I.C., 2019. Impact of internal control on fraud prevention in deposit money banks in Nigeria. *Nigerian Studies in Economics and Management Sciences*, *2*(1), pp.42-51.

[3] Ahmadi-Assalemi, G., Al-Khateeb, H., Epiphaniou, G., & Maple, C. (2020). Cyber resilience and incident response in smart cities: a systematic literature review. Smart Cities, 3(3), 894-927. https://doi.org/10.3390/smartcities3030046

[4] Aldribi, A. and Singh, A. (2022). Blockchain empowered smart home: a scalable architecture for sustainable smart cities. Mathematics, 10(14), 2378. https://doi.org/10.3390/math10142378

[5] Alfouzan, F. (2022). Augmented reality (AR) and cyber-security for smart cities—a systematic literature review. Sensors, 22(7), 2792. https://doi.org/10.3390/s22072792

[6] Algarni, A., Thayananthan, V., & Malaiya, Y. (2021). Quantitative assessment of cybersecurity risks for mitigating data breaches in business systems. Applied Sciences, 11(8), 3678. https://doi.org/10.3390/app11083678

[7] Alhalafi, N. and Veeraraghavan, P. (2021). Cybersecurity policy framework in saudi arabia: literature review. Frontiers in Computer Science, 3. https://doi.org/10.3389/fcomp.2021.736874

[8] Al-Turjman, F., Zahmatkesh, H., & Shahroze, R. (2019). An overview of security and privacy in smart cities' iot communications. Transactions on Emerging Telecommunications Technologies, 33(3). https://doi.org/10.1002/ett.3677

[9] Andrade, R., Yoo, S., Tello-Oquendo, L., & Ortiz-Garcés, I. (2020). A comprehensive study of the iot cybersecurity in smart cities. Ieee Access, 8, 228922-228941. https://doi.org/10.1109/access.2020.3046442

[10] Argaw, S., Troncoso-Pastoriza, J., Lacey, D., Florin, M., Calcavecchia, F., Anderson, D., … & Flahault, A. (2020). Cybersecurity of hospitals: discussing the challenges and working towards mitigating the risks. BMC Medical Informatics and Decision Making, 20(1). https://doi.org/10.1186/s12911-020-01161-7

[11] Auffret, J., Snowdon, J., Stavrou, A., Katz, J., Kelley, D., Rahman, R., … & Warweg, P. (2017). Cybersecurity leadership: competencies, governance, and technologies for industrial control systems. Journal of Interconnection Networks, 17(01), 1740001. https://doi.org/10.1142/s0219265917400011

[12] Avci, İ. (2021). Investigation of cyber-attack methods and measures in smart grids. Sakarya University Journal of Science, 25(4), 1049-1060. https://doi.org/10.16984/saufenbilder.955914

[13] Cavelty, M. (2014). Breaking the cyber-security dilemma: aligning security needs and removing vulnerabilities. Science and Engineering Ethics, 20(3), 701-715. https://doi.org/10.1007/s11948-014-9551-y

[14] Clim, A., Toma, A., Zota, R., & Constantinescu, R. (2022). The need for cybersecurity in industrial revolution and smart cities. Sensors, 23(1), 120. https://doi.org/10.3390/s23010120

[15] Cole, A. and Tran, E. (2022). Trust and the smart city: the hong kong paradox. China Perspectives, (2022/3), 9-20. https://doi.org/10.4000/chinaperspectives.14039

[16] Collen, A., Szanto, I., Benyahya, M., Genge, B., & Nijdam, N. (2022). Integrating human factors in the visualisation of usable transparency for dynamic risk assessment. Information, 13(7), 340. https://doi.org/10.3390/info13070340

[17] Cornelius, F., Rensburg, S., & Kader, S. (2022). The value of criminological theories in explaining cybersecurity in south african smart cities. International Annals of Criminology, 60(2), 220-240. https://doi.org/10.1017/cri.2022.12

[18] Dash, B. and Sharma, P. (2022). Role of artificial intelligence in smart cities for information gathering and dissemination (a review). Academic Journal of Research and Scientific Publishing, 4(39), 58-75. https://doi.org/10.52132/ajrsp.e.2022.39.4

[19] Deibert, R. (2018). Toward a human-centric approach to cybersecurity. Ethics & International Affairs, 32(4), 411-424. https://doi.org/10.1017/s0892679418000618

[20] Fabian, A.A., Uchechukwu, E.S., Okoye, C.C. and Okeke, N.M., (2023). Corporate Outsourcing and Organizational Performance in Nigerian Investment Banks. *Sch J Econ Bus Manag, 2023Apr*, *10*(3), pp.46-57.

[21] Gotlib, D., Kulisiewicz, T., Muraszkiewicz, M., & Olszewski, R. (2020). Multiagency modeling of transformation strategies towards sustainable smart cities. Applied Sciences, 10(3), 853. https://doi.org/10.3390/app10030853

[22] Habibzadeh, H., Nussbaum, B., Anjomshoa, F., Kantarcı, B., & Soyata, T. (2019). A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. Sustainable Cities and Society, 50, 101660. https://doi.org/10.1016/j.scs.2019.101660

[23] Hämäläinen, M. (2019). A framework for a smart city design: digital transformation in the helsinki smart city., 63-86. https://doi.org/10.1007/978-3-030-23604-5_5

[24] Ilugbusi, S., Akindejoye, J.A., Ajala, R.B. and Ogundele, A., 2020. Financial liberalization and economic growth in Nigeria (1986-2018). *International Journal of Innovative Science and Research Technology*, *5*(4), pp.1-9.

[25] Ismagilova, E., Hughes, L., Rana, N., & Dwivedi, Y. (2020). Security, privacy and risks within smart cities: literature review and development of a smart city interaction framework. Information Systems Frontiers, 24(2), 393-414. https://doi.org/10.1007/s10796-020-10044-1

[26] Jannat, A., Ilyas, A., Saeed, T., Iftikhar, A., Zahra, A., & Jafri, A. (2020). Exploration of solutions for smart cities: challenges in privacy and security.. https://doi.org/10.1109/inmic50486.2020.9318070

[27] Kalinin, M., Krundyshev, V., & Zegzhda, P. (2021). Cybersecurity risk assessment in smart city infrastructures. Machines, 9(4), 78. https://doi.org/10.3390/machines9040078

[28] Khan, Z., Abbasi, A., & Pervez, Z. (2019). Blockchain and edge computing–based architecture for participatory smart city applications. Concurrency and Computation Practice and Experience, 32(12). https://doi.org/10.1002/cpe.5566

[29] Kim, K., Alshenaifi, I., Ramachandran, S., Kim, J., Zia, T., & Almorjan, A. (2023). Cybersecurity and cyber forensics for smart cities: a comprehensive literature review and survey. Sensors, 23(7), 3681. https://doi.org/10.3390/s23073681

[30] Kumar, S. (2021). The missing piece in human-centric approaches to cybernorms implementation: the role of civil society. Journal of Cyber Policy, 6(3), 375-393. https://doi.org/10.1080/23738871.2021.1909090

[31] Latif, S., Driss, M., Boulila, ., Huma, Z., Jamal, S., Idrees, Z., … & Ahmad, J. (2021). Deep learning for the industrial internet of things (iiot): a comprehensive survey of techniques, implementation frameworks, potential applications, and future directions. Sensors, 21(22), 7518. https://doi.org/10.3390/s21227518

[32] Li, C., Liu, X., Dai, Z., & Zhao, Z. (2019). Smart city: a shareable framework and its applications in china. Sustainability, 11(16), 4346. https://doi.org/10.3390/su11164346

[33] Li, S. (2020). Editorial: zero trust based internet of things. Eai Endorsed Transactions on Internet of Things, 5(20), 165168. https://doi.org/10.4108/eai.5-6-2020.165168

[34] Mitton, N., Papavassiliou, S., Puliafito, A., & Trivedi, K. (2012). Combining cloud and sensors in a smart city environment. Eurasip Journal on Wireless Communications and Networking, 2012(1). https://doi.org/10.1186/1687-1499-2012-247

[35] Mouchou, R., Laseinde, T., Jen, T.C. and Ukoba, K., 2021. Developments in the Application of Nano Materials for Photovoltaic Solar Cell Design, Based on Industry 4.0 Integration Scheme. In *Advances in Artificial Intelligence, Software and Systems Engineering: Proceedings of the AHFE 2021 Virtual Conferences on Human Factors in Software and Systems Engineering, Artificial Intelligence and Social Computing, and Energy, July 25-29, 2021, USA* (pp. 510-521). Springer International Publishing.

[36] Neupane, C., Wibowo, S., Grandhi, S., & Deng, H. (2021). A trust-based model for the adoption of smart city technologies in australian regional cities. Sustainability, 13(16), 9316. https://doi.org/10.3390/su13169316

[37] Nguyen, D., Pathirana, P., Ding, M., & Seneviratne, A. (2019). Blockchain for secure ehrs sharing of mobile cloud based e-health systems. Ieee Access, 7, 66792-66806. https://doi.org/10.1109/access.2019.2917555

[38] Nikitas, A., Michalakopoulou, K., Njoya, E., & Karampatzakis, D. (2020). Artificial intelligence, transport and the smart city: definitions and dimensions of a new mobility era. Sustainability, 12(7), 2789. https://doi.org/10.3390/su12072789

[39] Pieroni, A., Scarpato, N., Nunzio, L., Fallucchi, F., & Raso, M. (2018). Smarter city: smart energy grid based on blockchain technology. International Journal on Advanced Science Engineering and Information Technology, 8(1), 298. https://doi.org/10.18517/ijaseit.8.1.4954

[40] Pollini, A., Callari, T., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., ... & Guerri, D. (2021). Leveraging human factors in cybersecurity: an integrated methodological approach. Cognition Technology & Work, 24(2), 371-390. https://doi.org/10.1007/s10111-021-00683-y

[41] Prasetyo, Y. and Habibie, I. (2022). Smart city architecture development framework (scadef). Joiv International Journal on Informatics Visualization, 6(4), 869. https://doi.org/10.30630/joiv.6.4.1537

[42] Prasetyo, Y. and Lubis, M. (2020). Smart city architecture development methodology (scadm): a meta-analysis using soa-ea and sos approach. Sage Open, 10(2), 215824402091952. https://doi.org/10.1177/2158244020919528

[43] Radoglou-Grammatikis, P., Sarigiannidis, P., Iturbe, E., Rios, E., Martinez, S., Sarigiannidis, A., ... & Ramos, F. (2021). Spear siem: a security information and event management system for the smart grid. Computer Networks, 193, 108008. https://doi.org/10.1016/j.comnet.2021.108008

[44] Raimundo, R. and Rosário, A. (2022). Cybersecurity in the internet of things in industrial management. Applied Sciences, 12(3), 1598. https://doi.org/10.3390/app12031598

[45] Schaffers, H., Komninos, N., Pallot, M., Trousse, B., Nilsson, M., & Oliveira, A. (2011). Smart cities and the future internet: towards cooperation frameworks for open innovation., 431-446. https://doi.org/10.1007/978-3-642-20898-0_31

[46] Shah, S., Seker, D., Rathore, M., Hameed, S., Yahia, S., & Draheim, D. (2019). Towards disaster resilient smart cities: can internet of things and big data analytics be the game changers?. Ieee Access, 7, 91885-91903. https://doi.org/10.1109/access.2019.2928233

[47] Uchechukwu, E.S., Amechi, A.F., Okoye, C.C. and Okeke, N.M., 2023. Youth Unemployment and Security Challenges in Anambra State, Nigeria. *Sch J Arts Humanit Soc Sci*, *4*, pp.81-91.

[48] Vincent, A.A., Segun, I.B., Loretta, N.N. and Abiola, A., 2021. Entrepreneurship, agricultural value-chain and exports in Nigeria. *United International Journal for Research and Technology*, *2*(08), pp.1-8.

[49] Wang, J., Jiang, C., Zhang, K., Quek, T., Ren, Y., & Hanzo, L. (2018). Vehicular sensing networks in a smart city: principles, technologies and applications. Ieee Wireless Communications, 25(1), 122-132. https://doi.org/10.1109/mwc.2017.1600275

[50] Zhao, Z. and Zhang, Y. (2020). Impact of smart city planning and construction on economic and social benefits based on big data analysis. Complexity, 2020, 1-11. https://doi.org/10.1155/2020/8879132