Privacy and Smart Cities: A Bibliometric Analysis

Xhimi Hysa[1][0000-0002-2279-6690], Gianluca Maria Guazzo[2][0000-0002-6063-0616], Vilma Çekani[2][0000-0003-1605-9261] and Pierangelo Rosati[3][0000-0002-6070-0426]

[1] Polis University, Tirana 1051, Albania
[2] University of Salerno, Via Giovanni Paolo II, 132, 84084 Fisciano SA, Italy
[3]University of Galway, University Rd, Galway, Ireland

xhimi_hysa@universitetipoli.edu.al
giguazzo@unisa.it
vcekani@unisa.it
pierangelo.rosati@universityofgalway.ie

Abstract. The growing adoption of smart cities technologies provides local governments with a unique opportunity to leverage a wide range of digital technologies to create more efficient and more effective digital services. Such services provide clear benefits for citizens in terms of accessibility within urban areas andoverall quality of life. However, smart cities applications tend to rely on citizens' generated data that is typically analysed to further improve service delivery. Thecollection and use of this data may raise potential privacy concerns for citizens as they are often unaware of how and where the data is stored, and how it will beused and protected. This paper presents a bibliometric analysis of the existing literature related to privacy and smart cities, provides a brief summary and the main topics that have been addressed in the academic literature. The findings from this study are of interest to academic researchers but could also inform localgovernments and policymakers' approach to smart cities technologies.

Keywords: Privacy, Smart cities, Bibliometric analysis, VOSviewer.

1 Introduction

Privacy is an ongoing concern for citizens in smart cities. Generally, smart cities are associated with better quality of life thanks to the use of technology-based solutions that can not only provide basic services to citizens but also improve their relationship with the government and contribute to sustainable development [1]. Information Communication Technologies (ICT) are key enablers for smart cities solutions as they pro-vide the means to capture, store and analyse large volume of data about a city's infrastructure and how it is used at any given time. Such information allows local governments to make more informed decisions and may lead to a more optimised and sustainable use of the existing infrastructure. However, the collection of a large volume of dataregarding citizens' behaviour around the city may give rise to privacy concerns as the extent of data being collected may not always viewed as appropriate and in line with existing privacy frameworks [2].

Powell [3] refers to "data cities" as smart technologies like transport systems, air quality, or closed-circuit television (CCTV) cameras that use, and generate vast amounts of data [4]. In addition, Al Nuaimi et al. [5] outline six operational issues re-related to data gathering that might undermine the successful development and deployment of smart cities applications, namely data sources, data and information sharing, data quality, security and privacy, cost, and population size. Li et al. [6] also point out that ubiquitous use of smartphones and other portable devices may lead to the over-collection of personal data when such devices are used to deliver "smart city" services via mobile apps, therefore, posing a significant security risk for citizens. Similarly, Martinez et al. [7] state that citizens perceive large scale data collection in smart cities as a potential threat to their privacy and, more specifically, in relation to their identity, search history and location. Van Zoonen [4] identifies four concerning areas among smart citizens living in smart cities, namely impersonal data, service purpose, personal data, and surveillance. While the first two were mostly considered as minor concerns, the last two tend to be related to high level of privacy concerns among citizens and consequently to high resistance when it comes to accepting the implementation of the smart city applications. Moreover, their study showed that particular technologies (e.g., smart parking, smart bin) and data usage (e.g., predictive policing, social media monitoring) may raise more prominent concerns than others due to their potential use for surveillance purposes. While privacy scholars have attempted to propose different solutions to mitigate these concerns including, for example, privacy-enhancing technologies (e.g., virtual private networks) [9] and transparency-enhancing technologies (e.g., black boxes) [10], it clearly emerges from both the academic and the public debate that the extent of potential resistance smart cities applications face due to privacy concerns ultimately depend on the type of technology used to collect data, the type of data being collected and how it will be used. This study aims to provide an overview of the existing literature on privacy and smart cities guided by the following research question:

RQ. What are the different clusters that emerged from the intersection between privacy and smart city?

2 Data and Methods

In this study, we present a bibliometric analysis of the existing literature addressing privacy in the context of smart cities. A bibliometric analysis is based on the application of quantitative techniques on bibliographic data to identify clusters of publications dedicated to specific sub-topics within a given research field and to create a visual representation of the relationship between such topics [11, 12, 13]. By leveraging a relatively large amount of data, this methodology, unlike a more traditional systematic literature review, allows for a deeper analysis of the literature and guarantees greater impartiality, transparency, and replicability of results [14].

In this study, we used VOSviewer to conduct the bibliometric analysis. This was implemented through four main steps:

Step 1 - Data Collection: the list of publications was sourced from the Scopus database. The raw list of publications was downloaded along with a series of additional

metadata (e.g., authors, abstracts, keywords, number of citations etc.). More specifically, we initially searched for all publications published between 2010 and 2022 that matched the following search string based on title, abstract and keywords: ("privacy" OR "surveillance" OR "dataveillance") AND ("smart cit*" OR "digital cit*"). Initially, the search yielded 3,517 results. The results were subsequently refined by retaining only published peer-reviewed journal articles written in the English language; finally, we filtered the remaining publications by topic – i.e., "Computer Science", "Engineering", "Social Sciences", "Energy", "Business, Management, and Accounting", "Environmental Science", "Decision Sciences", "Arts and Humanities" and "Economics, Econometrics and Finance". These steps were necessary in order to retain high quality publications that were fully relevant for the context of this study. The final list of publications consisted of 1,241 documents.

Step 2 – Data Cleaning: the title, abstract and keywords of each publication included in our final list was converted into a text corpus and normalised as per Bertello et al. [14]. More specifically, words with the same meaning but different spelling were matched together using a thesaurus to reduce matrix dimensionality. Similarly, and punctuation and hyphens were removed from the corpus to avoid noise in the data.

Step 3 - Similarity Matrix: a word co-occurrence matrix was constructed based on the words used in each of the publications included in our final list; publications are then grouped into clusters based on their text similarity as outlined in Van Eck et al. [10].

Step 4 - Bibliometric Map and Visualisation: the results of the analysis conducted in Step 3 were then visualised using a network graph that show the linkages between keywords and clusters. More specifically, nodes in the network represent selected keywords and edges represent the relationships between nodes [16, 17]. The position of such nodes with the graph depends on its frequency (i.e., the more central a node is, the more frequently the corresponding keyword appeared in the corpus) and the strength of the relationship among different nodes (i.e., the closer two nodes are in the graph, the more frequently they co-occur within the corpus) [18]. Finally, different clusters are represented by different colours for ease of interpretation.

3 Results and discussions

Fig. 1 provides an overview of the main results of our Bibliometric analysis and a visual representation of the clusters identified in the corpus. The network analysis identified six clusters; each of them consists of a group of publications focused on a specific topic and is visually represented by a different colour Fig. 1. The largest cluster consists of 16 publications and focuses on privacy challenges related to the adoption and use of cloud computing for smart cities applications (red cluster). The second-largest cluster consists of 13 publications and mostly focuses on the role of blockchain and the Internet of Things (IoT) in privacy protection (green cluster). The third-largest cluster consists of 11 publications and focuses on challenges to citizens' privacy (blue cluster). The yellow cluster only includes 9 publications and focusses on more technical cybersecurity topics. The purple cluster consists of 7 publications and mostly focuses on smart

mobility applications. Finally, the smallest cluster consists of only 6 publications and focuses on the use of homomorphic encryption for securing smart cities applications. Highlights from each of these clusters are presented in the following sections.

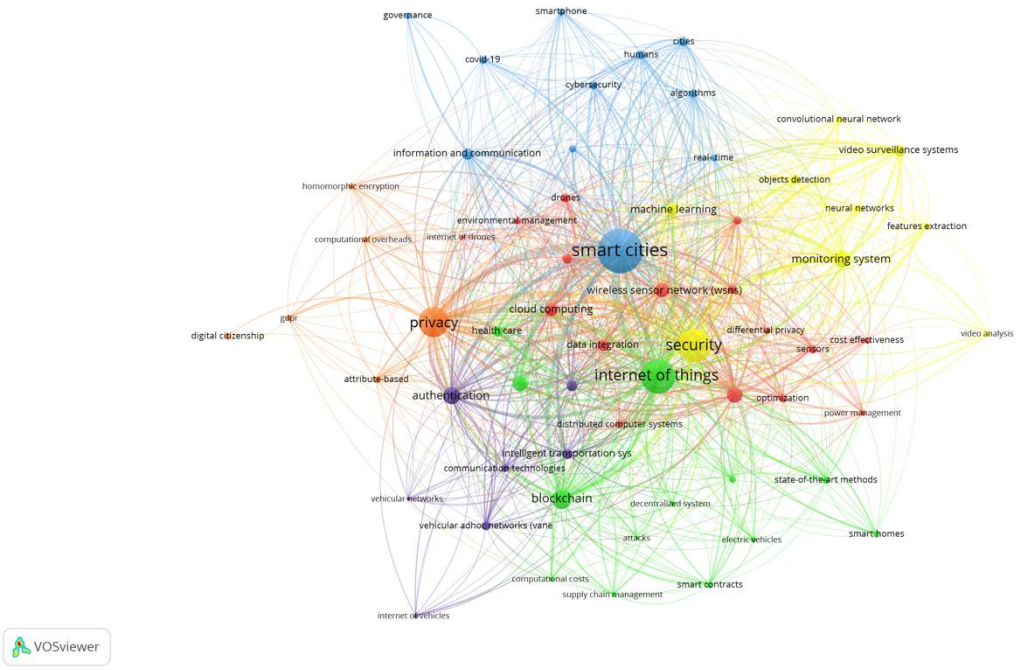

Fig. 1. Keywords co-occurrence map

3.1 Privacy challenges of cloud computing adoption for smart cities applications

The adoption and use of cloud computing is a key enabler of smart city applications but it also raises a number of challenges from a citizens' privacy perspective due to its distributed nature [20]. Unsurprisingly, this is the topic that has attracted the most attention from academic researchers. Squicciarini et al. [21], for example, focused on the problem of data loss and privacy in cloud computing and proposed a three-tier data protection architecture that leverages an innovative data binding technique to guarantee user privacy on the server side. Shen et al. [22], on the other hand, analysed the security requirements of cloud computing architectures; the authors suggest integrating cloud services for Trusted Computing Platform (TCP) and Trusted Platform Support Services (TSS) to build cloud models that users can trust. This is a necessary requirement for increasing the use of smart cities services powered by cloud computing. In this regard, Neisse et al. [23] suggest a system implemented on the Xen Cloud Platform using trusted computing technology to guarantee security.

3.2 Blockchain, IoT and privacy

The concepts of blockchain and IoT emerged as critical elements in the bibliometric analysis proposed in this study. Due to its decentralised, transparent, and secure nature, blockchain technology enables smart cities to adopt innovative solutions for data protection and regularity of transactions, i.e., data storage on distributed ledgers [24]. Makhdoom et al. [25], for example, proposed a blockchain-based framework called

"ProvySharing" for secure and privacy-friendly data sharing in smart cities. In this regard, Nguyen et al. [26] argue that blockchain may be used to preserve data privacy between cloud providers and IoT users during data exchange through a new framework resulting from the integration between blockchain and the Cloud of Things (CoT). This new framework, that the authors called "BCoT", enables reliable access control using blockchain-enabled smart contracts. These contracts automatically authorise operations of cloud providers and IoT devices, helping to prevent potential threats to cloud resources. In a similar fashion, Rahman et al. [27] presented a blockchain framework for secure smart city services that emphasises privacy and spatio-temporal smart contract services for IoT-enabled sharing economy solutions in urban areas. Furthermore, the use of blockchain technology to protect citizens' privacy has also been investigated in relation to the provision of smart medical services due to the susceptibility to cybercrime and mismanagement of patient data [28]. Other authors such as, for example, Kocabas and Soyata [29] and Dwivedi et al. [30] proposed a decentralised system that uses homomorphic encryption and zero-knowledge testing to safeguard sensitive health data while others (e.g., Malik et al. [28], Nguyen et al. [31] etc.) focused more on the integration of federated learning to the blockchain for improving the performance of digital medical services and protect patient privacy.

3.3 Challenges to citizens' privacy

It is well-established that one of the main objectives of smart cities applications is to improve the quality of life of citizens. With this perspective in mind, Cui et al. [32] and Angelidou [33] promote sustainable development of smart cities and propose different strategies that emphasise the role of ICT in enhancing urban systems' functionality, and in advancing knowledge transfer and innovation networks. The integration of big data, IoT infrastructures and sensor technology enables the development of urban interconnectivity and increases governmental efficiency through citizens' participation in the exchange of value [34, 35]. However, such hyper-connectivity may pose threats to the security and integrity of citizen data so systems need adequate security models to minimise the risk of unauthorised access and data vulnerability [32, 36]. Regarding the power system of smart cities, for instance, Alamaniotis et al. [37] emphasise the importance of privacy and security concepts in wireless network systems (WNSs), which enable the control of heat and light levels in smart cities and could be exposed to network attacks with possible repercussions on citizens' data. For this reason, more heterogeneity in the sources of data may reduce privacy risk while also improving the effectiveness of threat monitoring systems [38]. In this regard, Baig et al. [39] call for more research on how data is captured from, stored, and transmitted to infrastructures such as smart grids and unmanned aerial vehicles (UAVs).

3.4 Securing smart city applications

Security plays a key role in the context of smart cities as applications may collect a wide range of sensitive data from citizens and their social circles and automated processes may be in place to control different components of a city's infrastructure [40,

41]. Resource-constrained devices (e.g., smart sensors, smart street furniture etc.) make cities smart but, at the same time, vulnerable to various security attacks. This is due to the nature of such devices, and these vulnerabilities may lead to several cyberattacks in smart cities [42]. In this regard, Cui et al. [32] discuss a series of primary requirements that need to be addressed to make cities more secure and a series of technologies that may mitigate the impact of security attacks, such as cryptography, blockchain, and machine learning (ML). Luo et al. [43] propose a machine-based scheme for securing data detection and fusion in WSNs. Similarly, Aminanto et al. [44] developed a feature extraction and selection model based on ML for detecting attacks in Wi-Fi networks. Furthermore, new techniques for detecting and tracking objects have been developed thanks to advances in ML. In this regard, Elhoseny et al. [45] proposed an object detection model in real-time video surveillance systems, exploiting the Kalman optimal filtering technique. Again, Goyal et al. [46] use ML techniques based on the Viola-Jones algorithm to detect and classify real-time threats in video surveillance systems.

3.5 Smart mobility

The bibliometric analysis showed that privacy and security could be essential in the thematic concept of smart mobility within cities. Smart mobility and transportation represent crucial aspects within smart cities [47]. Smart mobility applications help improve traffic flow and gather feedback on city liveability and local public transport quality. Vehicular Ad-hoc Networks (VANETs) play a crucial role in this context, as each vehicle's movement generates significant data that can serve multiple purposes (e.g., traffic management, smart parking etc.). In their study, Pereira et al. [48] propose a Fog Computing architecture for deploying services in a VANET environment to detect traffic anomalies and estimate time of arrival for public transport. In VANETs, smart vehicles receive information from their surroundings; this information can be used to improve a wide range of services which may in turn provide practical benefits to citizens. This highlights the need to improve data quality while protecting the privacy of vehicle data providers and data/vehicle owners. In this regard, Li et al. [49] suggest a system called ATPS that considers trust and privacy to enhance the quality of data collection in VANETs while protecting data providers' privacy. At the same time, Di Maio et al.
[50] suggest the Software Defined Networking (SDN) paradigm as a possible solution to manage the threats VANETs are exposed to.

3.6 Data encryption

The privacy issue in the context of smart cities has attracted particular attention from scholars [4, 38]. Due to their hyper-connectivity, smart cities generate, process, analyse, share, and store a large amount of sensitive data; this leads to several concerns and challenges related to data privacy and how to protect it from unauthorised attacks. Indeed, the use of IoT, especially those with centralised control, is prone to vulnerabilities. In this regard, homomorphic encryption is a possible solution to overcome privacy issues, for instance, by allowing an untrusted third-party resource to process encrypted information without revealing confidential data. Rahulamathavan et al. [51] advocate

for the use of blockchain to guarantee privacy in IoT applications. The authors propose a new blockchain architecture for these applications based on attribute-based encryption (ABE) techniques. Similarly, Brabant et al. [52] propose a homomorphic cryptography framework to construct two privacy-preserving protocols and thus enable citizens to participate in democratic decision-making in cities. Gao et al. [53] instead leveraged homomorphic encryption and the design of secure network protocols to address the privacy-preserving problem for data auctions in cyber-physical systems (CPS) (e.g., smart city, smart grid, smart transportation, etc.).

4 Conclusions

This study provides a brief summary of the existing literature on privacy and smart cities. By implementing a bibliometric analysis, we showed that prior studies could be grouped into six main clusters as summarised in the previous sections. While it was not possible to present a more comprehensive analysis of the literature due to space limitations, our study aims to show that privacy in the context of smart cities is still a very timely topic in the academic literature and that such a topic can be tackled using a variety of approaches. In particular, this article suggests that privacy is a multidimensional concept that can be examined through different lenses, including legal, technological, ethical and social aspects. The clusters that emerged from our analysis suggest that academic research so far has mostly focused on some specific topics. While these have attracted most of the attention and effort so far, there are other perspectives that are still under investigation (e.g. legal implications, trust and acceptance etc.) and provide fruitful avenues for future research. However, the findings of our study are not of interest only to researchers. In fact, local and national policymakers may benefit from a better understanding of what the main privacy concerns of citizens are when it comes to designing and implementing smart city applications and services. As discussed by Troisi et al. [54], security and data governance are particularly relevant in this context.

As any study, the work presented in this manuscript is not free from limitations. First, our findings are based on publications sourced by a single database – Scopus. While this is arguably one of the most comprehensive repositories of academic publications, it does not feature all existing publications outlets and therefore a number of studies have been ignored. Furthermore, we limited our search criteria to peer-reviewed articles only, thus excluding conference papers, books, and book chapters. This was done to ensure that all publications included in our final list had gone through a formal peer review process but this is also implemented but a number of highly reputable conferences and book editors. Finally, the chosen methodology is limited to providing a descriptive analysis of the subject matter of the research. A more qualitative critical analysis of the literature may provide more detailed insights into the methodologies used across different clusters and highlight research gaps that may represent avenues for future research.

References

1. 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, 1-22 (2020).
2. Anisetti, M., Ardagna, C., Bellandi, V., Cremonini, M., Frati, F., Damiani, E.: Privacy-aware Big Data Analytics as a service for public health policies in smart cities. Sustainable cities and society, 39, 68-77 (2018).
3. Powell, A.: Datafication, transparency, and good governance of the data city. Digital enlightenment yearbook, 215-224 (2014).
4. Van Zoonen, L.: Privacy concerns in smart cities. Government Information Quarterly, 33(3), 472-480 (2016).

5. Al Nuaimi, E., Al Neyadi, H., Mohamed, N., Al-Jaroodi, J.: Applications of big data to smart cities. Journal of Internet Services and Applications, 6(1), 1-15 (2015).
6. Li, Y., Dai, W., Ming, Z., Qiu, M.: Privacy protection for preventing data over-collection in smart city. IEEE Transactions on Computers, 65(5), 1339-1350 (2015).
7. Martínez-Ballesté, A., Pérez-Martínez, P. A., & Solanas, A.: The pursuit of citizens' privacy: a privacy-aware smart city is possible. IEEE Communications Magazine, 51(6), 136-141 (2013).
8. Khan, Z., Pervez, Z., & Ghafoor, A.: 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing, pp. 806-811. IEEE (2014, December).
9. Rebollo-Monedero, D., Bartoli, A., Hernández-Serrano, J., Forné, J., Soriano, M.: (Reconciling privacy and efficient utility management in smart cities. Transactions on Emerging Telecommunications Technologies, 25(1), 94-108 (2014).
10. Beran, S., Pignotti, E., Edwards, P.: Trusted tiny things: Making devices in smart cities more transparent. In: Proceedings of the Fifth Workshop on Semantics for Smarter Cities-A Workshop at the 13th International Semantic Web Conference (ISWC 2014). CEUR-WS (2014, November).
11. Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., & Lim, W. M.: How to conduct a bibliometric analysis: An overview and guidelines. Journal of Business Research, 133, 285-296 (2021).
12. Broadus, R.N.: Toward a definition of “bibliometrics. Scientometrics 12(5–6):373–379) 1987).
13. Pritchard, A.: Statistical bibliography or bibliometrics. J. Doc 25(4), 348–349 (1969).
14. Bertello, A., De Bernardi, P., Ricciardi, F.: Open innovation: status quo and quo vadis-an analysis of a research field. Review of Managerial Science, 1-51 (2023).
15. Cobo, M. J., López-Herrera, A. G., Herrera-Viedma, E., Herrera, F.: An approach for detecting, quantifying, and visualizing the evolution of a research field: A practical application to the Fuzzy Sets Theory field. Journal of informetrics, 5(1), 146-166 (2011).
16. Van Eck, N., Waltman, L.: Software survey: VOSviewer, a computer program for bibliometric mapping. scientometrics, 84 (2), 523-538 (2010).
17. Van Eck N. J., L. Waltman L., van den Berg J., Kaymak U.: Visualizing the computational intelligence field [Application Notes]. IEEE Computational Intelligence Magazine, 1(4), 6-10 (2006). doi: 10.1109/MCI.2006.329702
18. De Bernardi P., Bertello A., Forliano C,. Orlandi L. B.: Beyond the “ivory tower”. Comparing academic and non-academic knowledge on social entrepreneurship.International Entrepreneurship and Management Journal,1–34 (2021).
19. Manesh M. F., Pellegrini, M. M., Marzi G., Dabic, M.: Knowledge management in the fourth industrial revolution: mapping the literature and scoping future avenues. IEEE Trans Eng Manage 68(1), 289–300 (2020).
20. Chen, D., Zhao, H.: Data security and privacy protection issues in cloud computing. In 2012 international conference on computer science and electronics engineering, vol. 1, pp. 647-651. IEEE (2012, March).
21. Squicciarini, A., Sundareswaran, S., Lin, D.: Preventing information leakage from indexing in the cloud. In: 2010 IEEE 3rd International Conference on Cloud Computing, pp. 188-195. IEEE (2010, July).
22. Shen, Z., Li, L., Yan, F., Wu, X.: Cloud computing system based on trusted computing platform. In: 2010 International Conference on Intelligent Computation Technology and Automation, vol. 1, pp. 942-945. IEEE (2010, May).

23. Neisse, R., Holling, D., Pretschner, A.: Implementing trust in cloud infrastructures. In: 2011 11th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, pp. 524-533. IEEE (2011, May).
24. Hakak, S., Khan, W. Z., Gilkar, G. A., Imran, M., Guizani, N.: Securing smart cities through blockchain technology: Architecture, requirements, and challenges. IEEE Network, 34(1), 8-14 (2020).
25. Makhdoom, I., Zhou, I., Abolhasan, M., Lipman, J., Ni, W. PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. Computers & Security, 88, 101653 (2020).
26. Nguyen, D. C., Pathirana, P. N., Ding, M., Seneviratne, A.: Integration of blockchain and cloud of things: Architecture, applications and challenges. IEEE Communications surveys & tutorials, 22(4), 2521-2549 (2020).
27. Rahman, M. A., Rashid, M. M., Hossain, M. S., Hassanain, E., Alhamid, M. F., Guizani, M.: Blockchain and IoT-based cognitive edge framework for sharing economy services in a smart city. Ieee Access, 7, 18611-18621 (2019).
28. Malik, R., Visvizi, A., Troisi, O., Grimaldi, M.: Smart services in smart cities: insights from science mapping analysis. Sustainability, 14(11), 6506 (2022).
29. Kocabaş, Ö., Soyata, T.: Medical data analytics in the cloud using homomorphic encryption. In E-Health and Telemedicine: Concepts, Methodologies, Tools, and Applications (pp. 751-768). IGI Global (2016).
30. Dwivedi, A. D., Srivastava, G., Dhar, S., Singh, R.: A decentralized privacy-preserving healthcare blockchain for IoT. Sensors, 19(2), 326 (2019).
31. Nguyen, D. C., Ding, M., Pham, Q. V., Pathirana, P. N., Le, L. B., Seneviratne, A., ..., Poor, H. V.: Federated learning meets blockchain in edge computing: Opportunities and challenges. IEEE Internet of Things Journal, 8(16), 12806-12825 (2021).
32. 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).
33. Angelidou, M.: (The role of smart city characteristics in the plans of fifteen cities. Journal of Urban Technology, 24(4), 3-28 (2017).
34. Alter, S.: Making sense of smartness in the context of smart devices and smart systems. Information Systems Frontiers, 22 (2), 381-393 (2020).
35. Polese, F., Troisi, O., Grimaldi, M., Loia, F.: Reinterpreting governance in smart cities: An ecosystem-based view. In: Smart Cities and the un SDGs, pp. 71-89. Elsevier (2021).
36. Troisi, O., Visvizi, A., & Grimaldi, M.: The different shades of innovation emergence in smart service systems: the case of Italian cluster for aerospace technology. Journal of Business & Industrial Marketing, (2021).
37. Alamaniotis, M., Tsoukalas, L. H., Buckner, M.: Privacy-driven electricity group demand response in smart cities using particle swarm optimization. In: 2016 IEEE 28th International Conference on Tools with Artificial Intelligence, ICTAI 2016, 946–953. IEEE (2017).
38. Nam, T., Pardo, T. A.: Smart city as urban innovation: Focusing on management, policy, and context. In: Proceedings of the 5th international conference on theory and practice of electronic governance, pp. 185-194. (2011, September).
39. Baig, Z. A., Szewczyk, P., Valli, C., Rabadia, P., Hannay, P., Chernyshev, M., ..., Peacock, M.: Future challenges for smart cities: Cyber-security and digital forensics. Digital Investigation, 22, 3-13 (2017).
40. Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., Shen, X. S.: (Security and privacy in smart city applications: Challenges and solutions. IEEE Communications Magazine, 55(1), 122-129 (2017).

41. Kashef, M., Visvizi, A., Troisi, O.: Smart city as a smart service system: Human-computer interaction and smart city surveillance systems. Computers in Human Behavior, 124, 106923 (2021).
42. Rashid, M. M., Kamruzzaman, J., Hassan, M. M., Imam, T., Gordon, S.: Cyberattacks detection in iot-based smart city applications using machine learning techniques. International Journal of environmental research and public health, 17(24), 9347 2020).
43. Luo, X., Zhang, D., Yang, L. T., Liu, J., Chang, X. Ning, H.: A kernel machine-based secure data sensing and fusion scheme in wireless sensor networks for the cyber-physical systems,'' Future Gener. Comput. Syst., 61, 85–96 (2016).
44. Aminanto, M. E., Choi, R., Tanuwidjaja, H. C., Yoo, P. D., Kim, K.: Deep abstraction and weighted feature selection for Wi-Fi impersonation detection. IEEE Trans. Inf. Forensics Security, 13(3), 621–636, (2018).
45. Elhoseny, M.: Multi-object detection and tracking (MODT) machine learning model for real-time video surveillance systems. Circuits, Systems, and Signal Processing , 39, 611-630 (2020).
46. Goyal, A., Anandamurthy, S. B., Dash, P., Acharya, S., Bathla, D., Hicks, D., ..., Ranjan, P.: Automatic border surveillance using machine learning in remote video surveillance systems. In: Emerging Trends in Electrical, Communications, and Information Technologies: Proceedings of ICECIT-2018, pp. 751-760. Springer, Singapore (2020).
47. Karger, E., Jagals, M., Ahlemann, F.: Blockchain for smart mobility—literature review and future research agenda. Sustainability, 13(23), 13268 (2021).
48. Pereira, J., Ricardo, L., Luís, M., Senna, C., Sargento, S.: Assessing the reliability of fog computing for smart mobility applications in VANETs. Future Generation Computer Systems, 94, 317-332 (2019).
49. Li, T., Xie, S., Zeng, Z., Dong, M., Liu, A.: ATPS: An AI based trust-aware and privacy-preserving system for vehicle managements in sustainable VANETs. IEEE Transactions on Intelligent Transportation Systems, 23(10), 19837-19851 (2022)..
50. Di Maio, A., Palattella, M. R., Soua, R., Lamorte, L., Vilajosana, X., Alonso-Zarate, J., Engel, T.: Enabling SDN in VANETs: What is the impact on security?. Sensors, 16(12), 2077 (2016).
51. Rahulamathavan, Y., Phan, R. C. W., Rajarajan, M., Misra, S., Kondoz, A.:. Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption. In: 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS). IEEE (2017, December).
52. Brabant, M., Pereira, O., Méaux, P.: Homomorphic encryption for privacy-friendly augmented democracy. In: 2022 IEEE 21st Mediterranean Electrotechnical Conference (MELECON), pp. 18-23. IEEE (2022, June).
53. Gao, W., Yu, W., Liang, F., Hatcher, W. G., Lu, C.: Privacy-preserving auction for big data trading using homomorphic encryption. IEEE Transactions on Network Science and Engineering, 7(2), 776-791 (2018).
54. Troisi, O., Fenza, G., Grimaldi, M., Loia, F.: Covid-19 sentiments in smart cities: The role of technology anxiety before and during the pandemic. Computers in Human Behavior, 126, 106986 (2022).