sustainability

MDPI

Editorial

Trust, Privacy and Security for Smart Cities

Yudong Zhang [1,2,*], Pushpita Chatterjee [3] and Amrit Mukherjee [4]

[1] School of Computing and Mathematic Sciences, University of Leicester, Leicester LE1 7RH, UK
[2] Department of Information Systems, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia
[3] Department of Electrical Engineering and Computer Science, Howard University, Washington, DC 20059, USA
[4] Institute of Applied Informatics, Department of Computer Science, University of South Bohemia, CZ-370 05 České Budějovice, Czech Republic
* Correspondence: yudongzhang@ieee.org; Tel.: +44-754-870-0453

The world is currently at the dawn of a new era characterized by a global transformation reshaping how we interact with our surroundings and each other. This global transformation is being fueled by rapid advancements in intelligent technologies [1,2], such as artificial intelligence (AI), big data, and the Internet of Things (IoT) [3,4]. These intelligent technologies increasingly connect people and their surrounding environments in previously unimaginable ways.

As we are witnessing the proliferation of these intelligent technologies, it is transparent that they hold tremendous promise for improving people's well-being and prosperity [5,6]. For example, these technologies help develop more efficient and sustainable systems for energy production, transportation, healthcare, and many other critical domains.

Future smart connected cities (FSCCs) [7] are urban areas that leverage advanced intelligent technologies to enhance their residents' quality of life while promoting the sustainable and efficient use of resources [8]. These cities utilize a wide range of technologies, such as the IoT, big data analytics, AI, and blockchain, to optimize the management of various city services, including transportation, energy, water, waste, public safety, and healthcare.

In FSCCs, these services are seamlessly integrated and connected through a robust digital infrastructure that enables real-time data collection and analysis. This allows city managers to make informed decisions and take proactive actions to improve the delivery of these services while also reducing waste.

Furthermore, the IoT-based smart city paradigm [9] is considered the latest wave of world information technology after the computer and the Internet. In an IoT-based smart city, various devices and sensors are deployed throughout the city to collect data on various parameters, such as traffic flow, air quality, energy consumption, waste management, and water usage. [10]. Different types of data are then analyzed in real-time to provide insights that enable city managers to make informed decisions and take proactive actions to improve the delivery of services, reduce waste, and minimize environmental impacts [11].

Nevertheless, with the proliferation of techniques in the smart city paradigm, many challenges emerge in achieving trust, privacy, interoperability, and security in the context of the smart city paradigm. The digital divide [12,13] is also important since smart city solutions may not be accessible to all citizens, particularly those from marginalized communities or areas with limited connectivity.

Meanwhile, trust, privacy, and security are critical to developing sustainable smart cities [14]. As cities become more connected and data-driven, ensuring the systems' trustworthiness and protecting citizens' privacy and security become increasingly important [15]. Smart city technologies can improve the quality of life for citizens, increase efficiency and sustainability, and drive economic growth. Still, these benefits are only possible if the systems are designed with trust, privacy, and security in mind [16]. Ensuring trust, privacy, and security in future sustainable smart cities is critical for several reasons.

Citation: Zhang, Y.; Chatterjee, P.; Mukherjee, A. Trust, Privacy and Security for Smart Cities. *Sustainability* **2023**, *15*, 5523. https://doi.org/10.3390/su15065523

Received: 15 March 2023
Accepted: 20 March 2023
Published: 21 March 2023

First, it promotes citizen confidence and participation in smart city initiatives, leading to greater acceptance and adoption of new technologies. Second, it protects citizen privacy and data, preventing potential abuses or misuse by third parties. Third, it safeguards critical infrastructure and systems from cyber-attacks [17,18], ensuring the continuity of essential services. Fourth, it fosters innovation by enabling secure and responsible data sharing between the public and private sectors. Finally, it promotes sustainable urban development by improving the efficiency of resource allocation [19] and reducing waste, resulting in more livable and resilient cities [20].

Ultimately, ensuring trust, privacy, and security in future smart cities is essential for creating sustainable and equitable urban environments that benefit all citizens. The successful development of sustainable smart cities depends on implementing robust measures to ensure trust, privacy, and security.

To achieve these objectives, technical solutions such as data encryption, access control, authentication, data minimization, anonymization, blockchain technology, and threat modeling can be employed [21]. Encryption can secure sensitive data, access control mechanisms ensure only authorized access [22], authentication verifies identities, data minimization limits data collection, anonymization removes personal identifiers, blockchain technology provides tamper-proof and decentralized records [23], and threat modeling identifies potential security threats [24]. A holistic approach that considers the entire smart city ecosystem is essential to safeguard citizen privacy and security while delivering the benefits of smart city technologies to enhance urban life [25].

This SI aims to bring together researchers from academia, industry, and government agencies to understand innovative technologies to achieve security and trust privacy in FSCCs. Submitted papers are expected to cover solutions using state-of-the-art and novel approaches for the smart city related to cost-effectiveness, security, sustainability problems, and challenges.

Author Contributions: All authors have read and agreed to the published version of the manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Deng, R.; Li, C.E. Digital intelligent management platform for high-rise building construction based on bim technology. *Int. J. Adv. Comput. Sci. Appl.* **2022**, *13*, 1057–1067. [CrossRef]
2. Zha, Y.P.; Wang, H.J.; Shen, Z.X.; Shi, Y.C.; Shu, F. Intelligent identification technology for high-order digital modulation signals under low signal-to-noise ratio conditions. *IET Signal Process.* **2023**, *17*, e12189. [CrossRef]
3. Subhan, F.; Mirza, A.; Su'ud, M.B.; Alam, M.M.; Nisar, S.; Habib, U.; Iqbal, M.Z. AI-enabled wearable medical internet of things in healthcare system: A survey. *Appl. Sci.* **2023**, *13*, 1394. [CrossRef]
4. Alizadehsani, R.; Roshanzamir, M.; Izadi, N.H.; Gravina, R.; Kabir, H.M.D.; Nahavandi, D.; Alinejad-Rokny, H.; Khosravi, A.; Acharya, U.R.; Nahavandi, S.; et al. Swarm intelligence in internet of medical things: A review. *Sensors* **2023**, *23*, 1466. [CrossRef]
5. Sakano, J.; Sawada, Y.; Okata, H.; Yajima, Y. Title: Sense of coherence as a mediator between social support and mental well-being amaong japanese elderly people. *Qual. Life Res.* **2022**, *31*, S127.
6. Rosales, R.J.J.; Adia, C.M.; Miral, K.C.M. The well-being and the will of the people amid COVID-19. *J. Public Health* **2022**, *44*, E602–E603. [CrossRef]
7. Valter, P.; Lindgren, P.; Prasad, R. The future role of multi-business model innovation in a world with digitalization and global connected smart cities. *Wirel. Pers. Commun.* **2020**, *113*, 1651–1659. [CrossRef]
8. Lavery, D.; Ruffini, M.; Valcarenghi, L.; Yoshimoto, N.; Pfeiffer, T.; Hood, D.; Zhang, J.W.; King, D.; Roberts, H.; Yadav, R.; et al. Networks for future services in a smart city: Lessons learned from the connected ofcity challenge 2017. *IEEE Commun. Mag.* **2018**, *56*, 138–144. [CrossRef]
9. Panagiotakopoulos, T.; Kiouvrekis, Y.; Misthos, L.M.; Kappas, C. Rf-emf exposure assessments in greek schools to support ubiquitous IoT-based monitoring in smart cities. *IEEE Access* **2023**, *11*, 7145–7156. [CrossRef]
10. Zeng, Y.Y.; Zhou, S.J.; Xiang, K. Online-offline interactive urban crowd flow prediction toward IoT-based smart city. *IEEE Trans. Serv. Comput.* **2022**, *15*, 3417–3428. [CrossRef]
11. Whaiduzzaman, M.; Barros, A.; Chanda, M.; Barman, S.; Sultana, T.; Rahman, M.S.; Roy, S.; Fidge, C. A review of emerging technologies for IoT-based smart cities. *Sensors* **2022**, *22*, 9271. [CrossRef]
12. Pettersson, L.; Johansson, S.; Demmelmaier, I.; Gustavsson, C. Disability digital divide: Survey of accessibility of ehealth services as perceived by people with and without impairment. *BMC Public Health* **2023**, *23*, 181. [CrossRef]

13. Yang, E.; Kim, M.J.; Lee, K.H. Digital divide and difficulties in acquiring health resources in disabled older adults during the pandemic. *Innov. Aging* **2022**, *6*, 797. [CrossRef]
14. Ghosh, U.; Chatterjee, P.; Shetty, S.S.; Kamhoua, C.; Njilla, L. Towards secure software-defined networking integrated cyber-physical systems: Attacks and countermeasures. In *Cybersecurity and Privacy in Cyber-Physical Systems*; CRC Press: Boca Raton, FL, USA, 2019; pp. 103–132.
15. Kovanic, M.; Spac, S. Conceptions of privacy in the digital era: Perceptions of slovak citizens. *Surveill. Soc.* **2022**, *20*, 186–201. [CrossRef]
16. Maiti, M.; Ghosh, U. Next-generation internet of things in fintech ecosystem. *IEEE Internet Things J.* **2023**, *10*, 2104–2111. [CrossRef]
17. Wan, Y.H.; Dragicevic, T. Data-driven cyber-attack detection of intelligent attacks in islanded dc microgrids. *IEEE Trans. Ind. Electron.* **2023**, *70*, 4293–4299. [CrossRef]
18. Al-Jarrah, O.Y.; El Haloui, K.; Dianati, M.; Maple, C. A novel detection approach of unknown cyber-attacks for intra-vehicle networks using recurrence plots and neural networks. *IEEE Open J. Veh. Technol.* **2023**, *4*, 271–280. [CrossRef]
19. Ji, Y.; Cai, H.C.; Wang, Z.L. Impact of industrial synergy on the efficiency of innovation resource allocation: Evidence from chinese metropolitan areas. *Land* **2023**, *12*, 177. [CrossRef]
20. Nawre, A. Fluid thinking for resilient livable cities an interview with herbert dreiseitl. *J. Archit. Educ.* **2020**, *74*, 144–148. [CrossRef]
21. Babu, E.S.; Kavati, I.; Cheruku, R.; Nayak, S.R.; Ghosh, U. Trust-based permissioned blockchain network for identification and authentication of internet of smart devices: An e-commerce prospective. *J. Interconnect. Netw.* 2243001. [CrossRef]
22. Saraswathy, K.S.; Sujatha, S.S. Using attribute-based access control, efficient data access in the cloud with authorized search. *Int. J. Electr. Comput. Eng. Syst.* **2022**, *13*, 569–575. [CrossRef]
23. Das, D.; Banerjee, S.; Chatterjee, P.; Ghosh, U.; Biswas, U. A secure blockchain enabled v2v communication system using smart contracts. *IEEE Trans. Intell. Transp. Syst.* **2022**. [CrossRef]
24. Chatterjee, P.; Ghosh, U.; Sengupta, I.; Ghosh, S.K. A trust enhanced secure clustering framework for wireless ad hoc networks. *Wirel. Netw.* **2014**, *20*, 1669–1684. [CrossRef]
25. Das, D.; Banerjee, S.; Dasgupta, K.; Chatterjee, P.; Ghosh, U.; Biswas, U. Blockchain enabled sdn framework for security management in 5g applications. In Proceedings of the 24th International Conference on Distributed Computing and Networking, Kharagpur, India, 4–7 January 2023; pp. 414–419.