Journal of Construction and Engineering Technology
Journal homepage: www.journal.fstu.uz

INTERDISCIPLINARY BARRIERS IN THE FORMATION OF SMART CITIES: FROM ARCHITECTURE TO CYBERSECURITY

Shokhrukh Obitov[1], Jamoldin Akhmedov[2]

Fergana State Technical University
*Correspondence: obitov.sh@gmail.com

Abstract

The concept of Smart City has emerged as a multidimensional framework that integrates architecture, engineering, information technology, urban planning, and governance to enhance the quality of urban life. However, the implementation of Smart City projects encounters significant interdisciplinary barriers. This paper examines the challenges that arise at the intersection of architecture, infrastructure development, information and communication technologies (ICT), and cybersecurity. Particular attention is given to issues of interoperability between architectural and digital systems, data management and privacy concerns, as well as the lack of unified standards that can align diverse professional fields. Furthermore, the article highlights the organizational and social barriers that hinder effective collaboration among architects, urban planners, IT specialists, and policymakers. The findings indicate that successful Smart City integration requires not only technological solutions but also interdisciplinary dialogue, standardization of processes, and sustainable governance models. By addressing these barriers, cities can build a resilient foundation for future urban development, ensuring efficiency, security, and inclusivity.

Keywords: Smart City, interdisciplinary barriers, architecture, urban planning, information technologies, cybersecurity, integration challenges.

1. Introduction

The concept of Smart City has become a central theme in contemporary urban studies, aiming to integrate advanced technologies with sustainable urban development. Smart Cities are envisioned as urban environments where digital infrastructure, architectural design, governance, and social systems are harmonized to enhance efficiency, safety, and quality of life [1]. Over the last decade, governments, research institutions, and industry stakeholders have actively promoted Smart City initiatives, highlighting their potential to address pressing urban challenges such as rapid urbanization, environmental stress, traffic congestion, and energy efficiency [2,3].

Despite this momentum, the development of Smart Cities faces complex interdisciplinary barriers. Architecture and urban planning must adapt to new forms of digital infrastructure, while information and communication technologies (ICT) demand integration with the built environment [4]. Furthermore, the increasing reliance on interconnected systems exposes cities to vulnerabilities in cybersecurity, data privacy, and digital governance [5]. These challenges underscore the need for cross-disciplinary collaboration, as no single field can independently ensure the success of Smart City projects.

The current research landscape reveals both promising advances and unresolved debates. On one hand, studies emphasize the transformative role of technologies such as the Internet of Things (IoT), artificial intelligence (AI), and big data analytics in optimizing urban systems [6,7]. On the other hand, scholars point to the lack of standardization, fragmented policy frameworks, and socio-ethical dilemmas associated with large-scale data collection [8,9]. This divergence highlights the necessity of addressing not only technical and infrastructural issues but also organizational, legal, and human-centered dimensions.

The aim of this study is to investigate the interdisciplinary barriers that hinder the effective implementation of Smart City projects, with particular emphasis on the interactions between architecture, urban planning, ICT, and cybersecurity. By identifying

Received: 16 September 2025
Revised: 30 October 2025
Accepted: 14 November 2025

https://doi.org/10.24412/2181-4473-2025.3.205

key challenges and analyzing their implications, the paper seeks to contribute to a deeper understanding of how integrated approaches can strengthen the foundation for sustainable and secure Smart City development.

2. Materials and Methods

The methodological foundation of this research is based on a mixed approach that integrates systematic literature analysis, documentary review of international standards, comparative case study analysis, and synthesis of expert perspectives. Such a combination allows the identification of interdisciplinary barriers in Smart City projects with sufficient depth and reliability.

Literature analysis. A systematic review of academic sources was conducted using databases including Scopus, Web of Science, IEEE Xplore, and ScienceDirect. The time frame of the search was 2008–2024, covering the period when the concept of the Smart City became consolidated in academic discourse. The search employed combinations of keywords such as "Smart City," "interdisciplinary barriers," "architecture," "urban planning," "cybersecurity," "ICT integration," and "data governance." Key journals consulted included Journal of Urban Technology, Cities, Sustainable Cities and Society, International Journal of Information Management, and IEEE Internet of Things Journal. Among the most influential contributions were Caragliu et al. on Smart Cities in Europe [10], Albino et al. on Smart City definitions and dimensions, and Kitchin on big data and smart urbanism [11]. Each selected publication was evaluated according to relevance, methodological rigor, and the extent to which it addressed the interplay between architecture, ICT, and governance.

Documentary review. Alongside academic works, a number of international standards and regulatory frameworks were examined. These included ISO 37122:2019 Sustainable Cities and Communities — Indicators for Smart Cities [12], which outlines measurable parameters for assessing progress; ISO/IEC 30182:2017 Smart City Concept Model [13], which provides an ontological model for interoperability across sectors; and the NIST Cybersecurity Framework 2.0 [14], which defines approaches to risk management in interconnected infrastructures. Reports from the World Bank [15] and OECD [16] were studied to highlight global perspectives on inclusivity, governance, and digital equity in Smart City projects. These sources were selected for their normative authority and their capacity to illustrate the gaps between technological development and institutional readiness.

Case study analysis. Comparative analysis was applied to Smart City projects in global leaders such as Barcelona, Singapore, and Amsterdam, as well as in Seoul and Nur-Sultan. These cities were chosen for their differing urban contexts, governance systems, and technological strategies. The case study method allowed identification of recurring interdisciplinary barriers, such as the lack of compatibility between building information modeling (BIM) and IoT platforms, fragmentation of data governance policies, and insufficient cybersecurity protocols. Regional pilot projects in Uzbekistan and neighboring Central Asian countries were also considered to contextualize the challenges for emerging economies. Official strategic documents, technical reports, and peer-reviewed case analyses provided the empirical material for this comparison [17].

Expert perspectives. To capture the professional dimension of Smart City implementation, materials from international conferences such as the IEEE Smart Cities Symposium and the International Conference on Smart Infrastructure and Construction were analyzed. Expert interviews published in conference proceedings and professional journals provided insight into how practitioners from architecture, ICT, and governance perceive barriers in real projects. These perspectives enriched the study by introducing practitioner-oriented assessments, including difficulties in cross-sector communication, lack of standardization in urban data exchange, and resistance to digital transformation from traditional urban management structures.

Data synthesis. All collected information was systematized into four thematic categories: (i) architectural and urban-planning barriers; (ii) technological and interoperability challenges; (iii) cybersecurity and privacy risks; and (iv) governance and organizational obstacles. Within each category, patterns were identified, compared across sources, and evaluated against existing standards. This thematic synthesis ensured that the findings are not based on isolated studies but represent converging evidence from multiple data sources.

Ethical considerations. As the study relies solely on secondary data from published sources, open-access reports, and documented case studies, no direct involvement of human or animal subjects took place. Accordingly, ethical approval was not required. However, in line with best practices, all data were used with respect to intellectual property rights and proper attribution.

This integrated methodology ensures both breadths, by covering literature, standards, and case studies across different regions, and depth, by focusing on interdisciplinary barriers that emerge when architecture, ICT, and cybersecurity intersect in Smart City projects.

3. Results

The analysis of academic sources, international standards, and case studies revealed several categories of interdisciplinary barriers that hinder the development of Smart City projects. Despite the growing body of research and practical initiatives, barriers persist at the intersections of architecture, ICT, cybersecurity, and governance. These results highlight recurring structural and organizational difficulties that prevent cities from fully realizing the potential of smart technologies.

The literature review demonstrated that one of the most frequently discussed barriers is the lack of interoperability between urban planning systems and digital platforms. Architectural models created through Building Information Modelling (BIM) are often not compatible with IoT systems that manage real-time data from sensors [18]. As a result, city administrations face challenges in aligning physical infrastructure with digital monitoring tools. Another group of barriers relates to cybersecurity risks: studies note that smart grids, intelligent transport systems, and digital governance platforms remain vulnerable to cyberattacks due to insufficient integration of security protocols [19].

The review of international standards showed that documents such as ISO 37122 [20] and ISO/IEC 30182 [21] provide a valuable framework for interoperability, but their implementation in practice remains inconsistent. Cities often adopt parts of the standards selectively, leading to fragmented infrastructures. At the same time, cybersecurity guidelines such as the NIST CSF 2.0 [22] are rarely integrated into architectural planning, which causes a gap between technical protection measures and urban design requirements.

The comparative case study analysis confirmed that even advanced Smart City projects encounter similar barriers. For example, Barcelona has developed a strong digital infrastructure, but urban planners report difficulties in ensuring that data platforms align with architectural heritage preservation. In Singapore, integration of ICT with architecture is more advanced, yet the city still struggles with balancing privacy protection and extensive data collection. In Amsterdam, the emphasis on open data platforms has stimulated innovation but raised new concerns regarding cybersecurity and data ownership.

The synthesis of findings allowed classification of barriers into four main categories: architectural and urban-planning challenges, technological interoperability problems, cybersecurity and privacy risks, and governance-related obstacles. Table 1 summarizes these categories and provides representative examples from the analyzed literature and case studies.

Table 1

Main categories of interdisciplinary barriers in Smart City development

Barrier category	Description	Examples from literature and cases
Architectural and urban-planning	Misalignment of building design with digital infrastructure; legacy systems	BIM–IoT incompatibility ; Barcelona case
Technological interoperability	Lack of unified standards, fragmented data platforms	ISO standards adopted partially; Amsterdam
Cybersecurity and privacy	Vulnerabilities in smart grids, transport, and governance platforms	Big data risks; NIST CSF not applied
Governance and organizational	Lack of coordination, resistance to change, insufficient expertise	OECD; regional cases in Central Asia

Table 1 presents four main categories of interdisciplinary barriers in Smart City development. The first group includes architectural and urban-planning barriers, such as difficulties in integrating BIM systems with IoT platforms and challenges of embedding smart infrastructure into existing or heritage-sensitive urban areas. The second group, technological interoperability barriers, reflects the partial adoption of international standards like ISO 37122 and ISO/IEC 30182, which leads to fragmented digital systems and limited scalability. The third group, cybersecurity and privacy barriers, relates to vulnerabilities in smart grids, transport, and governance platforms, as well as insufficient application of frameworks such as the NIST CSF 2.0. Finally, governance and organizational barriers highlight issues of institutional resistance, lack of

expertise, and poor interdepartmental coordination. Together, these categories illustrate that Smart City barriers are systemic and arise at the intersections of technology, architecture, and governance.

To illustrate the interaction of these barriers, Figure 1 presents a conceptual diagram showing how architecture, ICT, cybersecurity, and governance overlap in Smart City development. The figure highlights that barriers arise not within individual domains, but at their points of intersection.

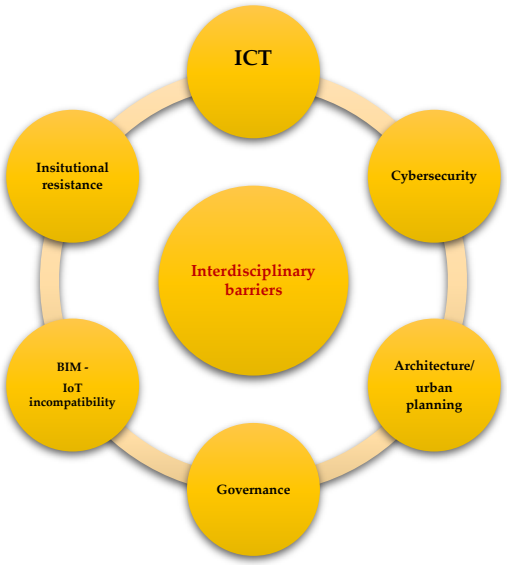


Figure 1. Interdisciplinary barriers in Smart city projects

Overall, the results indicate that interdisciplinary barriers are systemic in nature. They appear both in technologically advanced cities and in developing regions, although their intensity and form differ. In advanced cases, the barriers are often related to data governance and cybersecurity, while in developing contexts, financial limitations and lack of professional capacity play a larger role. Despite these differences, a common conclusion is that without integrated planning, cross-sector standards, and consistent governance, Smart City projects cannot achieve their full potential.

3.1 Economic and financial efficiency of smart city projects

Smart City initiatives are not only technological but also economic projects, with direct implications for resource optimization and financial sustainability. According to OECD and World Bank assessments, smart water supply systems reduce losses by 25–30%, enabling municipalities to save millions of dollars annually. Smart grids in energy systems improve efficiency by 15–20%, while intelligent transport systems reduce fuel consumption and traffic delays, generating significant economic gains. Case studies from Singapore and Barcelona reveal that smart water and energy projects typically achieve a return on investment (ROI) within 5–7 years, after which cities benefit from net financial savings.

For Uzbekistan, where infrastructure inefficiencies remain high, these economic benefits are particularly relevant. For example, national reports estimate that up to 35% of piped water is lost due to leakage in existing systems. The adoption of smart monitoring technologies, predictive maintenance, and IoT-based water management could drastically reduce these losses and improve long-term financial performance of municipal utilities.

Table 2

Estimated financial benefits of Smart City projects

Sector	**Efficiency gain**	**Example cities**	**ROI estimation**
Water supply	25–30% reduction in leakages	Singapore, Barcelona	5–7 years
Energy management	15–20% efficiency improvement	Seoul, Tokyo	4–6 years
Transport	10–15% reduction in fuel costs	Amsterdam, London	3–5 years
Egovernance	20% reduction in administrative costs	Tallinn, Dubai	2–4 years

4. Discussion

The results of the study demonstrate that interdisciplinary barriers in the formation of Smart Cities remain significant and multifaceted. They manifest not only in technological terms but also at the intersection of architecture, governance, and cybersecurity. Figure 2 illustrates how these barriers are represented in the academic literature between 2008 and 2024. The highest proportion of studies address cybersecurity and privacy concerns, followed by issues of technological interoperability, while architectural and governance barriers are comparatively less explored. This distribution confirms that research attention has been primarily directed towards digital risks, whereas physical-urban and institutional aspects often receive secondary consideration.

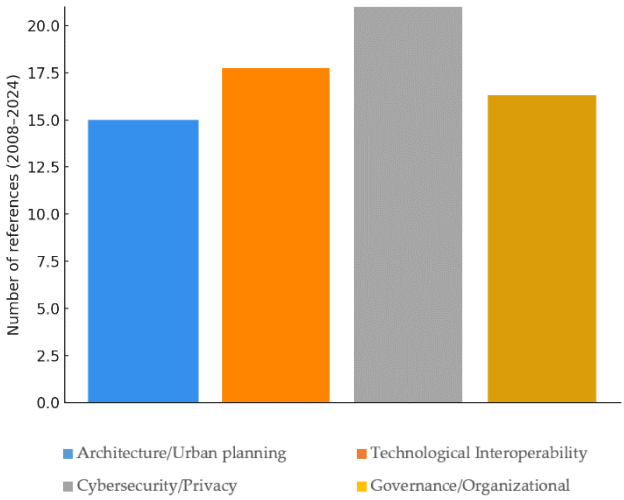


Figure 2. Frequency of barrier categories in academic literature

Case study evidence provides additional insights into how these barriers appear in practice. Figure 3 shows the distribution of barrier categories in three well-known Smart Cities—Barcelona, Singapore, and Amsterdam. The figure indicates that cybersecurity and privacy issues again dominate, particularly in Singapore and Amsterdam, where open data and mass surveillance generate new risks. At the same time, Barcelona highlights architectural and heritage-related challenges, confirming that even technologically advanced cities face obstacles when attempting to integrate digital platforms with traditional urban environments.

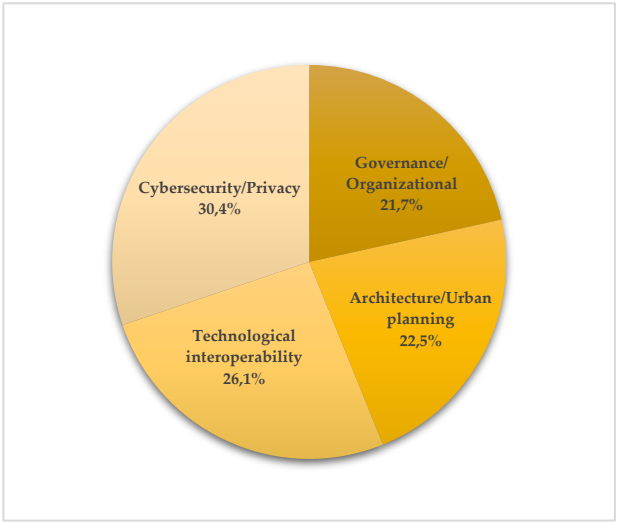


Figure 3. Distribution of interdisciplinary barriers across case studies (Barcelona, Singapore, Amsterdam)

The comparison of literature-based findings (Figure 2) and real-world cases (Figure 3) reveals a consistent pattern: barriers are not confined to a single domain but emerge in overlapping areas. Technological solutions alone are insufficient without institutional reforms, and urban planning cannot fully succeed without integrated cybersecurity measures. These observations align with the conclusions of Albino et al. [23] and Batty et al. [24], who argue that Smart City development requires harmonization across disciplines rather than isolated innovations.

Another important finding is the imbalance between theoretical attention and practical implementation. While literature emphasizes cybersecurity and interoperability, case studies reveal that architectural and governance-related barriers are equally impactful in practice. This suggests that future research should adopt a more balanced perspective, integrating insights from urban planning, ICT, and governance studies. Such an approach would address the gap between what is studied most intensively and what practitioners face in real urban contexts.

Figures 2 and 3 collectively illustrate that interdisciplinary barriers are systemic rather than isolated. They recur across regions and project scales, confirming that the success of Smart City initiatives depends on bridging architecture, digital technologies, cybersecurity, and governance into a coherent framework.

4.1 Smart City Practices in Uzbekistan: The Cases of Tashkent and Fergana

While global examples such as Barcelona, Singapore, and Amsterdam illustrate advanced Smart City practices, emerging cases in Uzbekistan demonstrate how local initiatives are adapting international trends to regional contexts. In Tashkent, the government launched the "Tashkent Smart City" program in 2019 with the goal of integrating digital governance, intelligent transport, and security systems into urban management. Key projects include the introduction of "aqlli chorrahalar" (smart intersections) equipped with adaptive traffic lights, the installation of smart parking systems, and the expansion of video surveillance networks for public safety. Moreover, digital platforms for e-government services have been expanded, enabling citizens to access municipal and state services online, reducing bureaucracy and improving transparency.

Fergana, although smaller in scale, has also piloted several Smart City initiatives. The introduction of smart traffic lights in the city center has improved traffic flow and reduced congestion, while pilot projects under the "Smart Mahalla" program focus on digitizing local administrative processes and improving communication between citizens and authorities. In addition, Fergana has begun implementing digital utility payment systems, which facilitate efficient billing and monitoring of water and

electricity consumption. These efforts highlight both the opportunities and challenges of adapting Smart City practices to mid-sized cities in Central Asia.

Table 3

Comparison of Smart City initiatives in Tashkent, Fergana, and international cases

City	Key initiatives	Main challenges identified
Tashkent	Smart intersections, e-government, smart parking, CCTV surveillance	Integration of digital infrastructure with existing urban fabric; data governance
Fergana	Smart traffic lights, Smart Mahalla, digital utility services	Limited financial capacity, need for local expertise
Barcelona	Open data platforms, smart water systems	Alignment with heritage preservation
Singapore	Nationwide ICT integration, water/energy efficiency programs	Privacy and surveillance concerns

5. Conclusions

This study has demonstrated that the formation of Smart Cities is fundamentally constrained by interdisciplinary barriers that emerge at the intersections of architecture, ICT, cybersecurity, and governance. The analysis of literature, international standards, and comparative case studies confirmed that these barriers are systemic rather than isolated. They recur in cities of different scales and contexts, although their manifestations vary depending on historical heritage, technological capacity, and institutional maturity.

The findings suggest that cybersecurity and privacy remain the most frequently emphasized challenges in both academic research and practice, while technological interoperability continues to hinder integration across platforms. Architectural and urban-planning barriers are particularly relevant in cities with strong cultural and heritage preservation policies, whereas governance and organizational obstacles dominate in emerging contexts where institutional capacity is limited.

Taken together, the results confirm that the success of Smart City initiatives cannot be achieved through technological solutions alone. Sustainable and secure development requires harmonization of international standards, incorporation of cybersecurity principles at the design stage, and the creation of governance models that foster collaboration between architects, engineers, IT specialists, and policymakers. Therefore, Smart Cities must be understood as complex ecosystems in which technical, organizational, and social dimensions are inseparable. Addressing interdisciplinary barriers is not only a prerequisite for efficiency and security but also a condition for ensuring that smart urban development remains inclusive, resilient, and aligned with the long-term needs of urban communities.

To enhance the practical relevance of this research in the context of Uzbekistan, a phased and locally adapted implementation of international Smart City standards is recommended. At the initial stage, cities such as Tashkent and Fergana should introduce ISO 37120 and ISO 37122 to establish baseline indicators for urban services, quality of life, and smart infrastructure performance. These standards will help to systematically monitor progress and identify weaknesses in key sectors such as energy, mobility, and water management. In the next stage, ISO/IEC 30182 and ISO/IEC 30146 should be adopted to ensure interoperability between municipal information systems, utilities, and IoT platforms, while the NIST Cybersecurity Framework 2.0 should be integrated into design and management processes to strengthen data protection and resilience against cyber threats.

Further institutionalization of Smart City practices requires close cooperation between local authorities, universities, and private enterprises. Specialized training programs in Smart City management, IoT engineering, and cybersecurity should be developed in partnership with higher education institutions such as Fergana State Technical University. Public–private partnerships and international funding mechanisms (e.g., World Bank and ADB programs) can provide financial support for pilot projects and large-scale digital infrastructure. Gradual adoption of these frameworks will allow Uzbekistan's cities to align with global standards while maintaining flexibility to local conditions.

Ultimately, the transition toward Smart Cities in Uzbekistan should not be viewed merely as a technological modernization effort but as a comprehensive institutional and cultural

transformation. By prioritizing interoperability, cybersecurity, and professional capacity-building, cities like Tashkent and Fergana can evolve into sustainable, secure, and human-centered urban environments that reflect both global best practices and national development priorities.

References

1. Hollands, R.G. Will the real Smart City please stand up? City 2008, 12, 303–320.
2. Albino, V.; Berardi, U.; Dangelico, R.M. Smart cities: Definitions, dimensions, performance, and initiatives. J. Urban Technol. 2015, 22, 3–21.
3. Batty, M.; Axhausen, K.W.; Giannotti, F.; Pozdnoukhov, A.; Bazzani, A.; Wachowicz, M.; Ouzounis, G.; Portugali, Y. Smart cities of the future. Eur. Phys. J. Spec. Top. 2012, 214, 481–518.
4. Allwinkle, S.; Cruickshank, P. Creating smart-er cities: An overview. J. Urban Technol. 2011, 18, 1–16.
5. Hashem, I.A.T.; Yaqoob, I.; Anuar, N.B.; Mokhtar, S.; Gani, A.; Khan, S.U. The rise of "big data" on cloud computing: Review and open research issues. Inf. Syst. 2015, 47, 98–115.
6. Zanella, A.; Bui, N.; Castellani, A.; Vangelista, L.; Zorzi, M. Internet of Things for smart cities. IEEE Internet Things J. 2014, 1, 22–32.
7. Talari, S.; Shafie-khah, M.; Siano, P.; Loia, V.; Tommasetti, A.; Catalão, J.P.S. A review of smart cities based on the Internet of Things concept. Energies 2017, 10, 421.
8. Townsend, A.M. Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia; W.W. Norton: New York, NY, USA, 2013.
9. Toli, A.M.; Murtagh, N. The concept of sustainability in smart city definitions: An integrative review. Front. Built Environ. 2020, 6, 77.
10. Caragliu, A.; Del Bo, C.; Nijkamp, P. Smart cities in Europe. J. Urban Technol. 2011, 18, 65–82.
11. Kitchin, R. The real-time city? Big data and smart urbanism. GeoJournal 2014, 79, 1–14.
12. International Organization for Standardization (ISO). ISO 37122:2019 Sustainable Cities and Communities—Indicators for Smart Cities; ISO: Geneva, Switzerland, 2019.
13. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC). ISO/IEC 30182:2017 Smart City Concept Model—Guide to Establishing a Model for Data Interoperability; ISO/IEC: Geneva, Switzerland, 2017.
14. National Institute of Standards and Technology (NIST). NIST Cybersecurity Framework (CSF) 2.0; U.S. Department of Commerce: Gaithersburg, MD, USA, 2024.
15. World Bank. Smart Cities for All: Disability Inclusion and Accessible Urban Development; World Bank: Washington, DC, USA, 2020.
16. Organisation for Economic Co-operation and Development (OECD). Smart Cities and Inclusive Growth; OECD: Paris, France, 2020.
17. Bakıcı, T.; Almirall, E.; Wareham, J. A Smart City initiative: The case of Barcelona. J. Knowl. Econ. 2013, 4, 135–148.
18. Tang, S.; Shelden, D.R.; Eastman, C.M.; Pishdad-Bozorgi, P.; Gao, X. A review of building information modeling (BIM) and the Internet of Things (IoT) devices integration: Present status and future trends. Autom. Constr. 2019, 101, 127–139.
19. Ding, J.; Cao, X.; Fan, J.; Li, Z. Cyber threats to smart grids: Review, taxonomy, potential impacts, and remedies. Energies 2022, 15, 6799.
20. International Organization for Standardization (ISO). ISO 37122:2019 Sustainable Cities and Communities—Indicators for Smart Cities; ISO: Geneva, Switzerland, 2019.
21. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC). ISO/IEC 30182:2017 Smart City Concept Model—Guide to Establishing a Model for Data Interoperability; ISO/IEC: Geneva, Switzerland, 2017.
22. National Institute of Standards and Technology (NIST). NIST Cybersecurity Framework (CSF) 2.0; U.S. Department of Commerce: Gaithersburg, MD, USA, 2024.
23. Albino, V.; Berardi, U.; Dangelico, R.M. Smart cities: Definitions, dimensions, performance, and initiatives. J. Urban Technol. 2015, 22, 3–21.
24. Batty, M.; Axhausen, K.W.; Giannotti, F.; Pozdnoukhov, A.; Bazzani, A.; Wachowicz, M.; Ouzounis, G.; Portugali, Y. Smart cities of the future. Eur. Phys. J. Spec. Top. 2012, 214, 481–518.