INJECT (Interdisciplinary Journal of Communication)
p-ISSN: 2548-5857; e-ISSN: 2548-7124
Vol. 11. No. 1 June 2026: p. 1199-1242
DOI: https://doi.org/10.18326/inject.v11i1.6585

Mapping Data Protection and Security in Smart Cities: A Systematic Mapping Study of Digital Communication Governance and Policy Frameworks

Muhammad Ikbal*
Program Studi Administrasi Publik, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Muhammadiyah Sidenreng Rappang, 91651, Sulawesi Selatan, Indonesia
iqbal.sidrap@yahoo.com

Herman Lawelai
Program Studi Ilmu Pemerintahan, Fakultas Ilmu Sosial dan Ilmu Politik Universitas Muhammadiyah Buton, Bau-Bau, 93724, Sulawesi Selatan, Indonesia
herman.lawelai@umbuton.ac.id

Achmad Nurmandi
Program Studi Ilmu Pemerintahan, Sekolah Tinggi Ilmu Pemerintahan Jusuf Kalla, Universitas Muhammadiyah Yogyakarta, 55711, Yogyakarta, Indonesia
nurmandi_achmad@umy.ac.id

Herman Dema
Fakultas Ilmu Sosial dan Ilmu Politik , Fakultas Ilmu Sosial dan Ilmu Politik , Universitas Muhammadiyah Sidenreng Rappang, 91651, Sulawesi Selatan, Indonesia
Hermandema1010@gmail.com

Elaine Macamay Baulete
Department of Political Science, Mindanao State University – Iligan Institute of Technology, Iligan City, 9200 Lanao del Norte, Philippines
elaine.baulete@g.msuiit.edu.ph

Abstract
This study examines policy directions for data protection and security in smart cities from a digital communication governance perspective by integrating

regulatory frameworks, technological innovations, and communication-based governance mechanisms to address emerging digital risks. A systematic mapping study guided by the PRISMA protocol was conducted using the Scopus database, covering publications from 2015 to 2024 and employing a comprehensive search strategy on smart cities, data protection, privacy, cybersecurity, data governance, and Internet of Things security. The study applies two complementary approaches: bibliometric mapping using RStudio-Biblioshiny and CiteSpace to identify thematic clusters, keyword citation bursts, and topic evolution, and qualitative policy-oriented synthesis of high-impact and highly relevant studies to translate bibliometric patterns into actionable policy insights. The findings reveal three dominant conceptual domains: technology ecosystems (e.g., IoT, artificial intelligence, blockchain), privacy-enhancing techniques (e.g., federated learning, differential privacy, cryptography), and regulatory and governance frameworks (e.g., GDPR compliance, consent management, and fundamental rights). From a communication perspective, these domains are closely linked to processes of digital information exchange, risk communication, transparency, and citizen engagement within smart city systems. The results demonstrate that effective data protection in smart cities depends not only on strong synergy between technical safeguards and policy governance, but also on how data-related risks and policies are communicated, understood, and trusted by the public. This study proposes a multi-level policy framework linking regulatory instruments, privacy-enhancing technologies, and institutional governance mechanisms, complemented by communication-based approaches such as transparency, risk communication, and public engagement, operating across city, national, and cross-border levels. The study contributes to smart city governance and communication literature by offering an explicit and integrative policy model that supports adaptive, citizen-centered, and sustainable data protection strategies in the digital age.

***Keywords**: Smart City, Data Protection, Digital Communication Governance, Risk Communication, Public Trust, Citizen Engagement*

1. Introduction

The rapid expansion of smart city initiatives has fundamentally reshaped urban governance through the integration of advanced information and communication technologies, including the Internet of Things (IoT), artificial intelligence, and big data analytics (Mishra & Chakraborty, 2020). From an interdisciplinary communication perspective, this transformation not only enhances public service delivery and efficiency but also reconfigures how information is produced, transmitted, and interpreted within digital urban environments. The large-scale collection and processing of personal and behavioral data within smart city ecosystems significantly increase risks related to data protection, privacy violations, and cybersecurity threats (Papaiakovou et al., 2022; Xia

et al., 2023), which are closely linked to processes of digital communication, risk perception, and information asymmetry between institutions and citizens. As urban systems become increasingly data-driven, ensuring the protection of sensitive information emerges not only as a technical and regulatory necessity but also as a communication challenge in maintaining public trust, transparency, and effective information exchange between governments and citizens. Despite these advancements, existing governance frameworks remain fragmented and reactive, creating a substantial mismatch between rapid technological innovation and the institutional capacity required to ensure effective data protection. Consequently, data protection in smart cities should no longer be treated solely as a technical issue, but as a complex communication-centered governance challenge that requires integrated regulatory, technological, institutional, and communication-based responses.

Existing literature on data protection in smart cities can generally be categorized into two dominant streams. The first stream emphasizes technological solutions, such as encryption, blockchain, and privacy-enhancing techniques, aimed at securing data within the system (V et al., 2024; Zhu et al., 2024). While these approaches significantly strengthen technical safeguards, they often overlook broader governance and communication dimensions, including accountability, institutional coordination, citizen rights, and the processes through which policies and risks are communicated to the public. The second stream focuses on regulatory and policy frameworks, including GDPR compliance, consent management, and data governance principles, which aim to protect individual rights and ensure accountability (Mondschein et al., 2021) (Stefanouli & Economou, 2019). However, these policy-oriented approaches often lack alignment not only with rapidly evolving technological developments but also with effective communication strategies, particularly in how data protection policies are disseminated, interpreted, and understood by stakeholders across different institutional contexts, resulting in fragmented and sometimes inconsistent data protection practices across jurisdictions (Hong et al., 2022). This divergence creates a structural tension between innovation-driven technological approaches and rights-based regulatory frameworks, which frequently operate under different priorities and institutional logics.

Beyond this dichotomy, recent studies highlight the increasing complexity of smart city ecosystems as socio-technical and socio-communication systems, where data protection involves interactions between infrastructure, that shape public understanding and engagement, algorithms, institutions, and societal values (Ha & Vu, 2024; Hong et al.,

2022). This perspective suggests that effective data protection requires not only technical security measures but also governance mechanisms that ensure transparency, accountability, and stakeholder coordination.

Despite the growing body of literature, a critical gap remains in integrating large-scale empirical knowledge mapping with policy-oriented and communication-oriented analysis. Existing bibliometric studies successfully identify research trends, thematic clusters, and topic evolution, but they rarely translate these findings into actionable governance frameworks. Conversely, policy-oriented studies frequently propose regulatory solutions without adequately addressing how these policies are communicated, perceived, and implemented within diverse stakeholder environments. This disconnect limits the ability to understand how technological advancements can be effectively aligned with governance mechanisms to address emerging data protection challenges in smart cities (Jin & Wang, 2025). As a result, there is limited guidance on how evidence-based research can inform coherent, implementable, and context-sensitive data protection policies in smart city governance.

To address this gap, this study adopts a theoretical perspective grounded in digital governance, multi-level governance, and digital communication governance. From this perspective, data protection in smart cities is conceptualized as a socio-technical governance issue that requires coordination between technological infrastructures, regulatory frameworks, and institutional actors operating at city, national, and cross-border levels (Ha & Vu, 2024; Hong et al., 2022). This approach emphasizes that effective data protection policies must not only rely on technical solutions but also on communication processes, including transparency, risk communication, and citizen engagement, to ensure accountability and trust in digital urban environments. This perspective extends existing governance approaches by explicitly linking technological systems with institutional and regulatory dynamics in complex, data-driven urban ecosystems.

This study aims to systematically map the development of research on data protection and security in smart cities from a digital communication governance perspective and to identify key thematic trends and governance challenges. Furthermore, this study develops a multi-level policy framework that integrates technological, regulatory, institutional, and communication dimensions that integrates technological, regulatory, and institutional dimensions to support effective, adaptive, and sustainable data protection strategies in smart city ecosystems (Vashishth et al., 2024).

The novelty of this study lies in its integrative approach that combines systematic mapping with policy-oriented and communication-

oriented synthesis to bridge the gap between knowledge production and policy design. Unlike previous studies that focus either on technological innovation or regulatory frameworks, this research introduces a policy-oriented bibliometric synthesis framework that systematically translates empirical research patterns into actionable governance and communication insights, particularly in understanding how data protection policies are communicated, interpreted, and operationalized within smart city ecosystems. By doing so, this study contributes to the development of adaptive, evidence-based, and citizen-centered data protection policies in the context of increasingly complex and interconnected smart city systems.

2. Method

This research employs a systematic review of existing literature, utilizing the Scopus database (Baas et al., 2020), to examine security and privacy in smart cities, with a particular focus on emerging trends, salient topics, and recent advances in research. This approach also enables interpretation of bibliometric patterns from a communication governance perspective. The selection of Scopus is based on its multidisciplinary coverage and content that is subject to peer review (Cortegiani et al., 2020). This database serves as the underlying framework, thus facilitating the identification of important themes in the security and transparency domain (Hughes-Noehrer et al., 2024).

In addition, this research also serves to synthesize existing literature related to artificial intelligence, blockchain technology, and data protection in smart cities (Baas et al., 2020)This research systematically evaluates existing research to identify knowledge gaps and synthesize the findings, resulting in a high-quality cross-cutting review that maps challenges and solutions to enhance security and privacy in smart cities.

2.1 Research Design and Data Source

This study employs a systematic mapping approach to examine the development of research on data protection and security in smart cities. The Scopus database was selected as the primary data source due to its comprehensive coverage of peer-reviewed and multidisciplinary publications, as well as its compatibility with bibliometric analysis tools (Baas et al., 2020). Scopus is widely recognized for ensuring data quality and consistency in large-scale literature analysis (Cortegiani et al., 2020). However, this study acknowledges that reliance on Scopus may exclude relevant grey literature, such as policy reports and governmental documents, which constitutes a limitation of the study.

2.2 PRISMA-Based Selection Process

This study follows the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework to ensure a transparent, systematic, and reproducible selection process (Haddaway et al., 2022; Moher et al., 2010). The selection process consists of four stages: identification, screening, eligibility, and inclusion. In the identification stage, a comprehensive search strategy was applied to retrieve relevant literature. The screening stage involved removing duplicate and irrelevant records, while the eligibility stage assessed full-text articles based on predefined inclusion and exclusion criteria. The final inclusion stage resulted in a refined dataset for bibliometric analysis. A structured search query was developed using a combination of title and keyword fields to ensure comprehensive coverage of the research domain. The search query applied in the Scopus database was:

> **TITLE-KEYWORDS ("data protection" OR "data privacy" OR "cybersecurity" OR "information security" OR "data governance" OR "IoT" OR "security" OR "trust" OR "identity management" OR "consent" OR "anonymization") AND ("smart city" OR "smart cities").**

This query was designed to capture both technological and governance dimensions of data protection in smart cities. The inclusion of multiple synonymous and related terms enhances search sensitivity, improves coverage, and minimizes the risk of omitting relevant studies, thereby strengthening the reliability and reproducibility of the analysis.

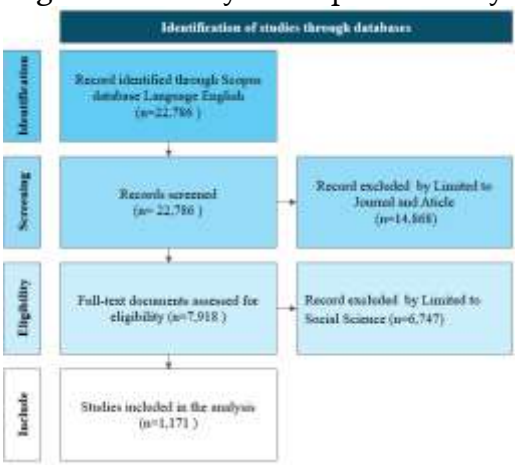

Figure 1. The detailed process of article selection based on the PRISMA framework is illustrated in Figure 1.

Source: Adapted from Wang et al. (2019) and produced using PowerPoint.

2.3 Inclusion and Exclusion Criteria

The inclusion criteria were defined to ensure relevance and quality of the selected studies. Articles included in this study were (1) published in peer-reviewed journals, (2) written in English, (3) focused on data protection, privacy, cybersecurity, or governance in smart cities, and (4) published within the period 2015–2024 to capture recent developments. Exclusion criteria included (1) non-English publications, (2) incomplete or inaccessible documents, (3) non-scholarly outputs such as editorials or short communications, and (4) studies lacking relevance to the research objectives.

2.4 Analytical Framework: From Bibliometric Mapping to Policy Insights

To address the limitation of purely descriptive bibliometric analysis, this study adopts an analytical framework that integrates bibliometric mapping with policy-oriented qualitative synthesis. The process consists of three stages. First, bibliometric analysis is conducted to identify thematic clusters, keyword co-occurrence, and citation bursts. Second, these patterns are interpreted to reveal relationships between technological developments, regulatory approaches, and governance mechanisms. Third, the interpreted findings are translated into policy insights by identifying governance gaps, regulatory needs, and institutional challenges. This framework enables a systematic linkage between empirical research patterns and policy formulation.

2.5 Data Analysis and Visualization Tools

This study utilizes two complementary bibliometric tools, namely RStudio-Biblioshiny and CiteSpace, to enhance analytical rigor (Lawelai, 2023). RStudio-Biblioshiny is employed to generate descriptive statistics, thematic maps, and keyword trends, allowing for the identification of dominant research themes (Chanduví et al., 2015). Meanwhile, CiteSpace is used to analyze temporal evolution, citation bursts, and conceptual structures, providing insights into the dynamic development of research topics (Xu et al., 2022). The combined use of these tools enables a more comprehensive understanding of both structural and temporal dimensions of the literature.

3. Results

3.1 Topic Trends of and Word Cloud

This study employs thematic mapping and word cloud visualization to systematically identify dominant research trends and keyword distributions in the field of data protection in smart cities. These analytical tools enable the detection of frequently occurring topics, their temporal

evolution, and their relative prominence within the literature. By integrating these visualization approaches, the study provides a structured empirical overview of how research themes develop and interact over time, thereby offering a clearer understanding of the intellectual landscape and emerging priorities in smart city data protection research.

Table 1. Trends, Topics in Data Protection, Topics in Smart Cities

Term	Frequency	Year (Q1)	Year (Median)	Year (Q3)
smart city	599	2020	2022	2024
internet of things	161	2020	2021	2023
internet	108	2021	2021	2023
sustainability	108	2021	2022	2024
sustainable development	100	2021	2022	2024
artificial intelligence	68	2021	2023	2024
network security	57	2020	2021	2022
data privacy	37	2018	2020	2022
china	36	2021	2024	2025
governance approach	36	2021	2024	2025

Source: Authors generated through RStudio-Biblioshiny

Table 1 demonstrates that "smart city" is the most dominant term (599 occurrences, median year 2022), followed by IoT, sustainability, and artificial intelligence. These results indicate that data protection research is structurally embedded within smart city development and is strongly associated with data-intensive infrastructures. The findings further show a consistent co-occurrence between technological terms and governance-related keywords, suggesting the increasing complexity of data protection issues in smart city systems. (Ahad et al., 2020; Allam & Dhunny, 2019)
The findings illustrate a clear causal mechanism in smart city systems: the expansion of IoT and artificial intelligence increases data generation, which subsequently amplifies privacy risks and cybersecurity vulnerabilities (Odeh et al., 2024). But extends prior studies by explicitly demonstrating how technological growth directly produces governance challenges. This causal linkage highlights that data protection issues are not incidental but structurally generated by data-driven infrastructures (Ha & Vu, 2024; Hong et al., 2022). The prominence of IoT and network security terms is consistent with previous studies (Mimo & McDaniel, 2022; Odeh et al., 2024), which highlight persistent privacy risks in digital

environments. The consistency of these findings indicates that such risks are structurally embedded within smart city systems rather than context-dependent.

However, unlike previous studies that primarily focus on technological efficiency, this study identifies a stronger integration between technological development and governance dimensions. The methodological approach used, which combines bibliometric mapping with policy-oriented synthesis, allows for a more comprehensive interpretation of both technical and institutional aspects of data protection. From an abductive perspective, technological innovation such as AI introduces new risks related to transparency and accountability, which require expanded regulatory responses. This finding aligns with studies emphasizing the importance of GDPR and similar frameworks in maintaining public trust and preventing data misuse (Shafik et al., 2024; Torre et al., 2019). Thus, governance mechanisms evolve in response to technological complexity, reinforcing the co-evolution of technology and regulation.

Figure 2. Word Cloud of Topics
Source: Authors generated through RStudio-Biblioshiny

Figure 2 presents the word cloud visualization highlighting the most frequently occurring keywords, including "smart city," "artificial intelligence," "cybersecurity," "privacy," "IoT," and "blockchain." The

distribution indicates a strong concentration of research themes around technological infrastructures and data security mechanisms. The relative size of each keyword reflects its frequency, showing the dominance of technology-oriented topics in the literature on smart city data protection. (Somanathan Pillai et al., 2025).

The dominance of these terms indicates that data protection is increasingly embedded within technological architectures, reflecting a strong technology-centric orientation in current research. However, this study identifies a critical limitation, as governance-related dimensions such as accountability, consent, and citizen rights receive comparatively less attention. This finding extends previous research (A. Kumar et al., 2022) by demonstrating that technological solutions alone are insufficient, and that effective data protection requires integration with governance mechanisms, including regulatory frameworks and institutional coordination. Therefore, effective data protection policies must integrate technical safeguards with institutional governance mechanisms to ensure transparency, legitimacy, and public trust in smart city systems.

From a practical perspective, these findings suggest that policymakers should adopt integrated approaches that combine privacy-by-design principles, regulatory frameworks, and institutional coordination. This includes establishing data governance units, enforcing compliance mechanisms, and integrating privacy-enhancing technologies to ensure accountability and public trust in smart city systems (Sharma & Mishra, 2024). The reliance on continuous data collection, while improving efficiency and sustainability, simultaneously increases exposure to privacy risks and cyber threats. Therefore, policymakers should implement adaptive regulatory mechanisms and institutional coordination strategies to ensure that technological innovation does not compromise citizen rights.

In addition, technological enablers such as the Internet of Things (IoT), artificial intelligence, and blockchain appear prominently, reflecting their growing role in shaping data-driven urban systems. IoT supports real-time data acquisition from sensors and connected devices, which requires strong protection against misuse. At the same time, blockchain offers potential for enhancing data integrity and security through its decentralized and immutable architecture (Sefati et al., 2024). These trends emphasize the increasing need for robust data protection strategies that leverage advanced technologies while preserving individual privacy in an evolving digital ecosystem (Medková, 2024).

3.2 Conceptual Structure Map and Keywords with the Strongest Citation Bursts

The conceptual structure map provides a visual representation of the relationships among key concepts in the literature on data protection in smart cities. Using correspondence analysis, this map identifies clusters of related themes and reveals the structural organization of knowledge within the field. By mapping these relationships, the analysis highlights how different research domains are interconnected and how thematic priorities evolve over time. This approach enables a systematic understanding of the intellectual structure underlying smart city data protection research and identifies dominant as well as emerging conceptual areas.

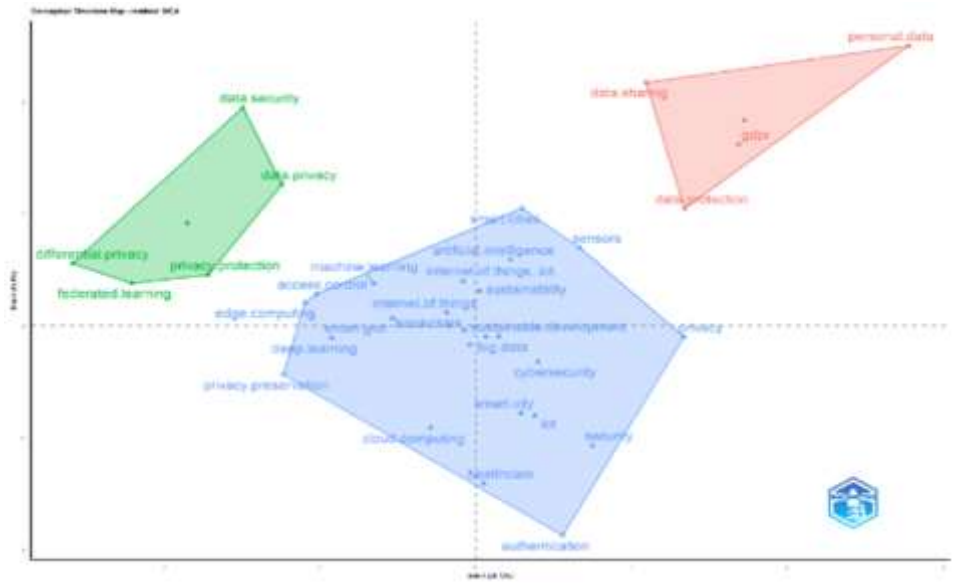

Figure 3. Conceptual Structure Map of Topics
Source: Authors generated through RStudio-Biblioshiny

Figure 3 reveals three major conceptual clusters that define the intellectual structure of data protection research in smart cities. The first cluster (blue) focuses on smart city ecosystems, including themes such as artificial intelligence, urban planning, sustainability, and decision-making. The second cluster (red) represents cybersecurity and data protection infrastructures, including IoT, blockchain, cryptography, and authentication systems. The third cluster (green) highlights computational intelligence approaches, including machine learning, optimization, and

detection algorithms, reflecting the increasing use of advanced analytics in data protection systems.

These clusters reflect the theoretical perspective of socio-technical systems, where technological infrastructures, analytical capabilities, and governance mechanisms interact dynamically. (Bhardwaj et al., 2022). The findings indicate a causal integration: smart city applications generate data, cybersecurity infrastructures protect this data, and computational intelligence enhances data processing and risk detection. This interdependence suggests that data protection cannot be addressed through isolated technical solutions, but requires integrated governance approaches that align technological innovation with institutional and regulatory frameworks.

The prominence of the cybersecurity cluster is consistent with previous studies emphasizing the importance of secure infrastructures in smart city systems (Hossain et al., 2024). However, unlike prior research that tends to treat cybersecurity as a purely technical issue, this study reveals its close integration with governance and application domains.

The emergence of the computational intelligence cluster highlights the growing role of machine learning and artificial intelligence in enhancing data protection systems. From an inductive perspective, these findings suggest an expansion of existing governance frameworks, where data protection increasingly relies on predictive and automated mechanisms. This extends prior literature by demonstrating that data protection is no longer limited to static regulatory compliance but involves adaptive and intelligent systems capable of responding to dynamic threats in real time. These topics reflect the growing use of intelligent analytical techniques to enhance system performance, anomaly detection, and privacy-preserving data processing in smart cities.

The integration of these three clusters implies that effective data protection policies must operate across multiple dimensions, combining application contexts, cybersecurity infrastructures, and advanced analytical methods. Practically, this means that policymakers should design integrated frameworks that align technological systems with regulatory standards and institutional coordination. This finding contributes to the literature by providing an empirically grounded model that links technological development with governance mechanisms, thereby addressing the fragmentation identified in previous studies. Such integration is essential to balance technological innovation, regulatory compliance, and technical privacy protection (Lnenicka et al., 2025; Padrão et al., 2024; Sun & Wu, 2020).

Table 3. Top 17 Keywords with the Strongest Citation Bursts

Keywords	Strength	Begin	End	2015 - 2025
Security of Data	6.74	2015	2019	
Electric Power Transmission Networks	6.91	2016	2020	
Distributed Computer Systems	3.78	2016	2018	
Big Data	16.86	2017	2018	
Trusted Computing	6.56	2017	2019	
Data Mining	4.28	2017	2019	
Smartphones	3.87	2017	2018	
Ubiquitous Computing	12.24	2018	2019	
Social Networking (Online)	4.26	2018	2019	
Data Communication Systems	14.45	2019	2020	
Internet of Things (IoT)	5.06	2019	2021	
Data Science	4.49	2019	2020	
Privacy By Design	10.62	2020	2021	
Intelligent Transportation	4.01	2020	2021	
Sensitive Data	7.47	2022	2025	
Block Chain	6.06	2022	2025	
Privacy Preserving Techniques	3.93	2022	2025	

Source: Authors generated through CiteSpace

Table 3 presents the keywords with the strongest citation bursts, indicating rapidly growing research attention over time. Early bursts are associated with terms such as “big data,” “trusted computing,” and “data mining,” while more recent bursts highlight “sensitive data,” “blockchain,” and “privacy-preserving techniques.” This temporal shift reflects changing research priorities from foundational data infrastructures toward more advanced and user-centered data protection approaches. In

the era of city digitization, data from IoT devices is used to manage energy distribution, monitor infrastructure, and manage electricity loads in real-time (Blumenthal, 2021; K. S. Kumar et al., 2022; Wu et al., 2020). However, this reliance on communication infrastructure also opens up potential security vulnerabilities. Smart grids, as the energy backbone of smart cities, face threats such as false data injection and ransomware that not only risk data integrity but can also cause service disruptions and even widespread outages if attacks target the electricity transmission network (Naeem et al., 2025; Wu et al., 2020).

This evolution aligns with prior studies emphasizing the transition from system-oriented security to privacy-centered governance approaches (Sefati et al., 2024; Zhu et al., 2024) Unlike earlier research focusing primarily on infrastructure protection, current trends prioritize safeguarding sensitive data and ensuring user privacy. This shift can be explained by the increasing volume of personal data generated by smart city systems, which requires more sophisticated protection mechanisms beyond traditional security frameworks.

This finding supports the argument that data protection evolves in response to both technological advancements and societal expectations, reinforcing the need for adaptive governance frameworks that can accommodate emerging risks and ethical considerations. The increasing attention to privacy-preserving technologies such as federated learning and blockchain indicates a growing effort to balance data utility with privacy protection (Sefati et al., 2024; Zhu et al., 2024). From a practical perspective, these findings suggest that policymakers should integrate emerging technologies such as blockchain and federated learning into regulatory frameworks to enhance data protection.

Besides security, privacy issues are also a major concern, especially in two-way communication schemes between users and energy providers. Real-time recorded electricity consumption patterns can provide an in-depth picture of individual activities, which, if leaked or misused, can threaten the privacy of citizens (Verma et al., 2022; Wu et al., 2020). Therefore, technological approaches such as federated learning based on differential privacy, as well as security architectures based on cyber-physical systems, are starting to be implemented to protect data while maintaining the continuity of electricity services intelligently (Li et al., 2024; Yan & Kunhui, 2024). In the framework of smart cities, data security and energy networks cannot be separated, as they synergistically determine how protected the system and privacy of urban communities are from contemporary digital threats.

Security and privacy in smart cities rely heavily on the protection of sensitive data, the implementation of blockchain and privacy-protecting techniques. Personal data from IoT devices must be guarded against misuse (Alshmrany, 2025; Vimercati et al., 2022). Blockchain offers secure and unmanipulable data logging (Mezquita et al., 2023; Padma & Ramaiah, 2024) while Federated Learning enables model training without moving data from local devices (Sefati et al., 2024; Zhu et al., 2024)(Samanta & Sarkar, 2025). This combination strengthens the overarching smart city privacy and security framework (P. Kumar et al., 2021; Raza et al., 2024), making it a key solution in the urban digital ecosystem.

3.3 Clusters by references, Timeline, topic evolution, and Thematic Evolution Map

This study utilizes cluster analysis, timeline visualization, and thematic evolution mapping to provide a comprehensive overview of the development of data protection and security research in smart cities. The cluster-by-references approach groups studies based on citation proximity, enabling the identification of dominant thematic areas. The timeline visualization illustrates the temporal dynamics of these clusters, while thematic evolution mapping captures the transformation and interconnection of research topics over time. Together, these methods provide a structured representation of how knowledge in this field evolves and expands. The Thematic Evolution Map visually maps the relationships between themes, systematically showing integration and future research directions.

Table 4. Summary of the largest 7 clusters by references.

ID	Size	Silhouette	Label (LLR)	Average Year
1	43	0,991	smart cities (32.61, 1.0E-4)	2019
2	39	0,983	privacy solution (30.27, 1.0E-4)	2015
5	31	0,971	cyber-secured smart cities (37.67, 1.0E-4)	2019
11	18	0,961	fundamental right (30.31, 1.0E-4)	2017
19	11	0,981	gdpr consent management (18.83, 1.0E-4)	2021
26	7	0,995	evidence from Chinese cities (10.12, 0.005)	2021
30	5	0,996	smart city solution (14.68, 0.001)	2020

Source: Authors generated through CiteSpace

Table 4 identifies several dominant clusters, with the largest cluster focusing on "smart cities," followed by clusters related to "privacy solutions," "cyber-secured smart cities," and "fundamental rights." These clusters indicate that research in this field is organized around three major dimensions: technological systems, privacy protection mechanisms, and normative governance frameworks. The presence of clusters such as "GDPR consent management" further highlights the increasing institutionalization of regulatory approaches within smart city data protection discourse. Followed by Cluster #2 (LLR: privacy solutions, 30.27), which highlights technical and policy approaches in protecting personal data, including the application of GDPR and the concept of privacy by design in smart city architecture (Mohamed et al., 2020; Sánchez Alcón et al., 2015). Cluster #11 (LLR: fundamental right, 30.31) emphasizes the ethical and human rights dimensions, particularly against the use of surveillance technologies such as facial recognition, which increasingly blur the line between security and privacy violations (Mobilio, 2023). Other clusters, such as #19 (gdpr consent management) and #30 (smart city solutions), contribute to the understanding of regulatory systems and real solutions in smart cities, strengthening the relevance of regulations and case studies to the implementation of citizen rights-based security.

From a theoretical perspective, these findings support the multi-level governance framework, where data protection operates across technological, regulatory, and institutional dimensions (Ha & Vu, 2024; Hong et al., 2022).. The coexistence of clusters related to privacy solutions, cybersecurity, and fundamental rights suggests that data protection is not a single-layer issue but a multi-dimensional governance challenge. This reinforces the argument that effective smart city governance requires coordination between technical systems, legal frameworks, and institutional actors operating at different levels. This finding extends previous studies. (Mohamed et al., 2020; Sánchez Alcón et al., 2015), which primarily treat technological and regulatory dimensions separately. In contrast, this study reveals that these dimensions coexist but remain insufficiently integrated. This gap can be attributed to differences in disciplinary approaches, where technical studies prioritize system efficiency, while policy studies emphasize legal compliance and rights protection. As a result, the lack of integration creates inconsistencies in implementing data protection across smart city systems.

This study contributes by providing empirical evidence that supports the need for integrated policy frameworks combining technical standards, legal instruments, and ethical considerations. Practically, this

implies that policymakers should design cross-sectoral governance mechanisms that align cybersecurity infrastructure with human rights principles. Such integration is essential to ensure that data protection policies are not only operationally effective but also socially legitimate and aligned with fundamental rights in smart city ecosystems.

Cluster #5, with the LLR label revised to cyber-secured smart cities (1.72), shows an in-depth focus on city infrastructure designed from the outset with cybersecurity and privacy risk mitigation in mind. The scope of this cluster includes an integrative study of technical standards, data security, and the design of smart city service systems that are resilient to cyberattacks and data manipulation (Vandercruysse et al., 2024). In this context, the cyber-secured design approach not only ensures the protection of energy infrastructure and communication networks but also integrates the principles of accountability, public participation, and protection of citizens' digital rights. Linking the findings from this cluster to the research agenda on smart city security and privacy, it is clear that digitally resilient city architecture relies heavily on collaborative governance and system design that takes into account both systemic and social risks.

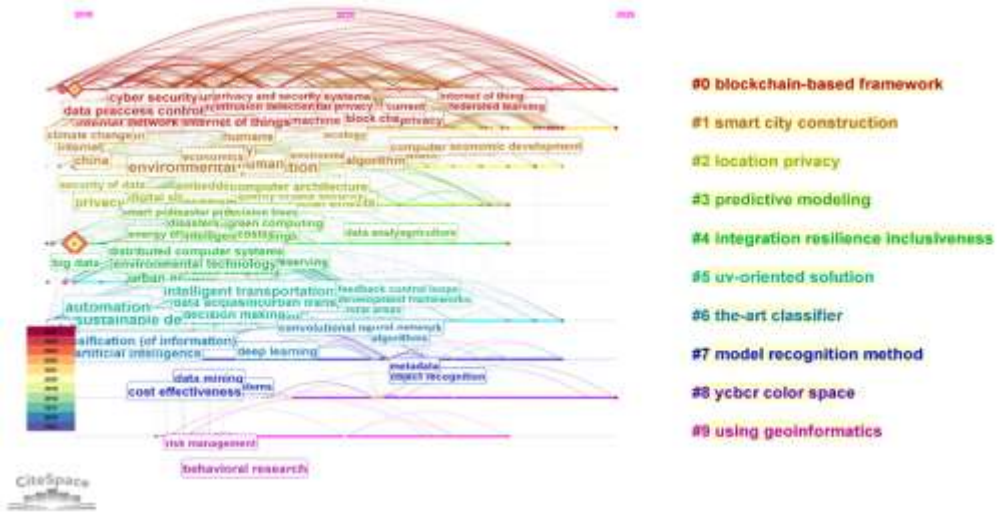

Figure 4. Timeline view of topic evolution
Source: Authors generated through CiteSpace

Figure 4 illustrates the temporal evolution of research clusters, revealing the emergence and development of key topics over time. The analysis identifies multiple clusters, including blockchain-based frameworks, location privacy, predictive modeling, and smart city integration systems. The timeline demonstrates that earlier research

focused on infrastructure and system development, while more recent studies emphasize privacy protection, cybersecurity resilience, and data governance mechanisms, indicating a shift toward more complex and integrated research priorities, which were analyzed using bibliometric visualization techniques such as burst detection, betweenness centrality, and LLR (Log-Likelihood Ratio) based clustering. The increasing prominence of blockchain-based frameworks reflects a causal response to growing concerns over data integrity and decentralization in smart city systems (Khan et al., 2024; Padma & Ramaiah, 2024). However, unlike earlier research that focuses primarily on technical capabilities, this study demonstrates that blockchain adoption is closely linked to broader governance challenges, including transparency, accountability, and cross-sector coordination. (Khan et al., 2024; Padma & Ramaiah, 2024). The use of blockchain has a high burst value, driven by a combination of keywords such as privacy by design and data-sensitive, as well as nodes such as smart cities (158 cities) (158 sites), data privacy (176), and network security (119), which are all featured in this cluster, confirming the importance of decentralized architecture in urban digital security.

Clusters #1 to #5 focus on urban computing frameworks and smart city integrative systems. The evolution of clusters related to urban systems, privacy protection, and predictive modeling reflects an increasing integration of technological and governance dimensions. From an abductive perspective, these findings indicate that smart city systems evolve through continuous interaction between technological innovation and governance adaptation. This suggests that emerging technologies not only create new capabilities but also generate new governance requirements, reinforcing the dynamic and co-evolutionary nature of smart city data protection systems. Cluster #1 (smart city construction) emphasizes the physical and environmental construction of ICT-based smart cities with strong topics such as environmental protection, pollution, and pollution control (Dincă et al., 2022; Q. Wang & Liu, 2024). Meanwhile, cluster #2 (location privacy) highlights digital watermarking techniques and privacy protection models in intelligent transportation systems and energy consumption, for example, through k-correlation privacy techniques and ontology-based data management (Sayah et al., 2021; Sui et al., 2017). Cluster #3 (predictive modeling) intertwines smart power grids with air quality prediction and energy management (Baran et al., 2016; Y. Wang & Kong, 2019), including the topic "electric power transmission networks" with a significant burst score (6.91), which bridges data security and energy infrastructure. Clusters #4 and #5 address the theme of integration, resilience, and inclusiveness, with the articulation of

smart city systems (health, transportation, environment) through big data-based evaluation methods and the universal village model (Z. Yang et al., 2020; Zhang et al., 2020).

The other clusters (#6-#9) underline technical approaches and advanced applications in data protection. Cluster #6 (for deep neural network watermarking) explores artificial intelligence and activity classification in smart homes (Nef et al., 2015; Y. Yang et al., 2018). Cluster #7 focuses on new differential privacy and federated learning, and the introduction of distributed models, such as federated learning, in city monitoring (Angus et al., 2022). Cluster #8 brings a visual dimension with color watermarking techniques in the YCbCr color space for the visual identity protection of urban citizens (Roldan et al., 2019), while cluster #9 introduces the utilization of geoinformatics to understand spatial behavior and urban risk and risk benefits (Jat & Saxena, 2018; Lv et al., 2018). All of these clusters emphasize that security and privacy rest not only on technological infrastructure, but also on smart integration between systems, management of sensitive data, and protection of citizens' rights in data-driven city ecosystems.

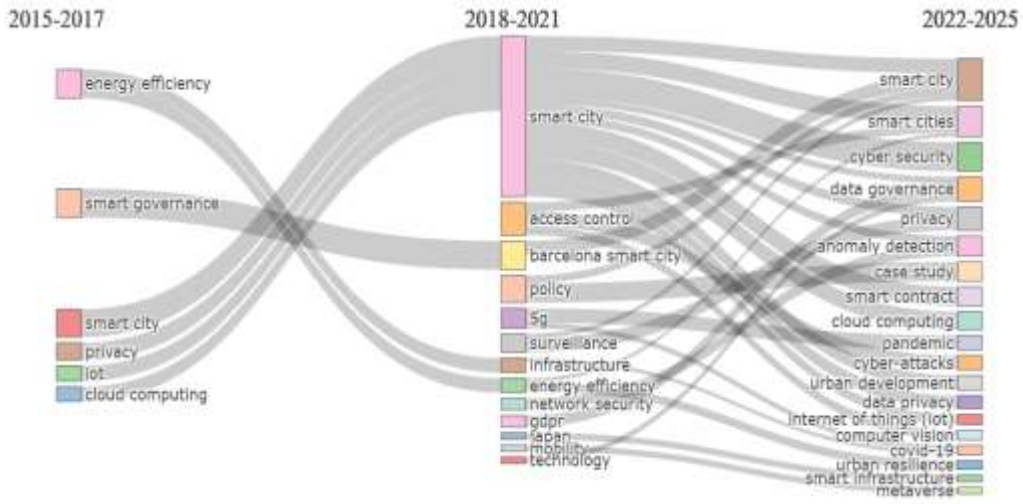

Figure 5. Thematic evolution of Topics
Source: Authors generated through RStudio-Biblioshiny

Figure 5 presents the thematic evolution of research on smart cities and data protection from 2015 to 2025. The early phase (2015–2017) is dominated by foundational themes such as IoT and smart cities. The intermediate phase (2018–2021) shows diversification into cybersecurity,

blockchain, and privacy protection. The most recent phase (2022–2025) demonstrates consolidation around key issues such as cybersecurity, interoperability, and sustainable development, indicating the maturation of the research field. In the early period (2015–2017), the thematic structure is dominated by foundational concepts such as "smart cities", "Internet of Things (IoT)", and "sustainability". During this stage, themes related to privacy and regulation, including "data privacy", "privacy protection", and "GDPR", begin to emerge, indicating early recognition of data protection implications alongside the initial expansion of smart city initiatives (Chhabra & Jaglan, 2024). Policy orientations in this phase remain exploratory, primarily preparing regulatory and institutional frameworks to accommodate evolving data protection norms (Srivastava & Sharifi, 2022).

This progression supports previous studies (Priya Dharshini et al., 2022) that identify a shift from technology-driven research toward governance-oriented approaches. However, this study extends existing literature by providing a more structured and evidence-based explanation of this transition. From a theoretical perspective, this reflects a shift from a techno-centric paradigm to a governance-centric model, where data protection is increasingly understood as a socio-technical challenge requiring adaptive regulatory and institutional responses (Angelini et al., 2020; Franke & Gailhofer, 2021). From a practical perspective, these findings suggest that policymakers must adopt adaptive and forward-looking regulatory frameworks that can respond to rapidly evolving technological risks. Future research should explore how these evolving themes are implemented in real-world governance contexts, particularly in developing countries where institutional capacities may vary significantly.

In the subsequent period (2018–2021), the map demonstrates substantial thematic diversification and deepening, reflecting intensive technological development. The "smart city" theme continues to function as a central anchor, while security- and privacy-oriented technical themes such as "cybersecurity", "blockchain", "homomorphic encryption", "encryption", and "differential privacy" gain prominence. Simultaneously, more specific application-oriented themes emerge, including "smart mobility", "energy efficiency", and "location privacy", indicating a growing concern with embedding privacy and security considerations into concrete smart city use cases (Ogunkan & Ogunkan, 2025).

In the most recent period (2022–2025), thematic consolidation is evident around core technologies such as "IoT" and "smart cities", key application domains, and systemic challenges including "cybersecurity",

"interoperability", and "sustainable development" (Priya Dharshini et al., 2022). Although certain privacy-related technical terms do not form independent dominant themes, the continued presence of "cybersecurity", "location privacy", and the emergence of "cyberattacks" confirm that data protection remains a persistent and critical concern. Consequently, contemporary and future policy approaches must be adaptive and responsive to evolving threat landscapes and technological change (Angelini et al., 2020; Franke & Gailhofer, 2021).

Table 5. Top 10 Citasi Teratas terhadap security and privacy in smart cities

Author	Issued Discuss	Findings	Number Citation
Hashem et al. (Hashem et al., 2016)	The role of big data in smart city	The integration of big data and IoT is the main foundation for smart city development, supported by cutting-edge communication technology, data analytics, and new business models, but it still faces significant challenges in terms of technology and business governance.	947
Allam & Dhunny (Allam & Dhunny, 2019)	On big data, artificial intelligence, and smart cities	Artificial intelligence and big data have great potential to improve urban design and management, but must be integrated with cultural, metabolic, and	935

Author	Issued Discuss	Findings	Number Citation
		governance dimensions to ensure sustainability and improve the quality of urban life.	
Dagher et al.(Dagher et al., 2018)	Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology	The use of blockchain technology through the Ethereum-based Ancile framework can improve the security, interoperability, and access control of electronic medical records, while balancing patient privacy needs with accessibility for healthcare providers.	783
Bibri (Bibri, 2018)	The IoT for smart sustainable cities of the future: An analytical framework for sensor-based big data applications for environmental sustainability	IoT-based big data applications play an important role in promoting urban environmental sustainability through smart resource and infrastructure management, but still face technological and integration challenges in	667

Author	Issued Discuss	Findings	Number Citation
		sustainable urban planning.	
Hammi et al. (Hammi et al., 2018)	Bubbles of Trust: A decentralized blockchain-based authentication system for IoT	Blockchain-based decentralized bubbles of trust systems are capable of providing authentication, identification, and protection of IoT data integrity mechanisms that are secure, efficient, and low-cost compared to centralized approaches.	637
Allam et al. (Allam et al., 2022)	The Metaverse as a Virtual Form of Smart Cities: Opportunities and Challenges for Environmental, Economic, and Social Sustainability in Urban Futures	The metaverse has the potential to revolutionize urban design and service provision through the integration of smart technologies, but it poses ethical, social, and cultural challenges to the quality of sustainable urban living.	540

Author	Issued Discuss	Findings	Number Citation
Moustafa (Moustafa, 2021)	A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets	The distributed IoT testbed architecture generates a heterogeneous and realistic TON_IoT dataset and has been proven effective in validating the high performance of machine learning algorithms in detecting IoT network security threats.	535
Ahad et al.(Ahad et al., 2020)	Enabling technologies and sustainable smart cities	Supporting technologies such as IoT, AI, and WSN are the main foundations of smart cities, but their development faces technical, socio-economic, and environmental challenges that require mitigation strategies and best practices towards sustainability.	524

Author	Issued Discuss	Findings	Number Citation
Javed et al. (Javed et al., 2022)	Future smart cities requirements, emerging technologies, applications, challenges, and future aspects	The development of future smart cities depends on the integration of various cutting-edge technologies, accompanied by significant challenges, requiring new frameworks and dimensions to realize sustainable cities with a priority on smart living.	519
Singh et al. (Singh et al., 2020)	Convergence of blockchain and artificial intelligence in IoT networks for the sustainable smart city	The convergence of blockchain and AI has the potential to build a sustainable smart city ecosystem, but its success is highly dependent on addressing security issues and developing appropriate solutions and guidelines.	485

Source: Scopus Database 2025

Table 5 shows that the core literature on smart cities consistently places big data, IoT, and artificial intelligence as the main foundations of smart city building. The study of (Allam & Dhunny, 2019; Hashem et al., 2016) asserts that the integration of big data–IoT–AI enables improved quality of public services, urban planning, and resource management, but at the same time poses serious challenges related to security, privacy, and data governance. (Bibri, 2018) (Ahad et al., 2020) reinforces this argument

by showing that sensor-based big data applications contribute greatly to environmental sustainability, but face technical barriers and complex system integration. From a policy perspective, these findings indicate the need for regulatory instruments that require the application of privacy-by-design, data minimization, and risk-based data governance principles in every smart city project, both through national data protection laws and sectoral technical guidelines.

The next group of articles highlights the role of distributed technology and security architecture as an operational means of data protection. Dagher et al. (Dagher et al., 2018) and Hammi et al. (Hammi et al., 2018) show that blockchain is able to provide stronger authentication mechanisms, access control, interoperability, and data integrity protection than centralized approaches. Mustafa (Moustafa, 2021) and Singh et al. (Singh et al., 2020) Expand on these findings by emphasizing the importance of distributed architecture and blockchain–AI convergence in detecting IoT security threats in real-time. The policy implications of this study group are directly related to technical standard instruments, such as the adoption of IoT security standards, blockchain-based system certification, and security auditing obligations on smart city infrastructure. In addition, a public procurement policy is needed that requires the use of technology that meets security and privacy standards.

Meanwhile, the article by Allam et al. (Allam et al., 2022) and Javed et al. (Javed et al., 2022) shifting the discourse towards the social, ethical, and governance dimensions of the future of smart cities, including the potential of the metaverse, sustainability challenges, and the need for new policy frameworks. Their findings emphasize that technical solutions alone are not enough without clear institutional coordination between the central government, municipal governments, the private sector, and communities. Thus, additional relevant policy instruments include the establishment of urban data governance units, public-private collaboration mechanisms, and public participation channels in data policy formulation. Overall, the comparison of these ten key articles shows that the direction of smart city data protection policies should be multi-level and integrated, combining strong regulations, clear technical standards, effective institutional governance, and citizen engagement as key pillars.

Table 6. Top 5 articles based on relevance to security and privacy in smart cities

Author	Issued Discuss	Findings
Sefati et al. (Sefati	Cybersecurity issues, data	The BFLIoT framework, which integrates blockchain and federated

Author	Issued Discuss	Findings
et al., 2024)	privacy, and scalability in smart city IoT infrastructure.	learning, can improve the security, scalability, efficiency, and privacy of IoT data in smart cities, while reducing the risk of data leaks and system latency.
Semenov et al. (Semenov et al., 2025)	The issue of UAV communication security vulnerabilities and ADS-B data protection.	The Fourier transform-based steganography method significantly improves the security of ADS-B UAV data, reduces signal distortion, and strengthens the resilience of UAV communications in supporting sustainable smart city operations.
Naili et al. (Naili et al., 2024)	Isu perlindungan privasi data pasien dan kepatuhan terhadap regulasi IoT.	The existing legal framework provides the basis for IoT-based health data protection, but technical regulations are still needed to ensure effective and balanced implementation in smart city practices.
Eskridge (Eskridge, 2019)	Issues of privacy governance, data security, and surveillance risks.	Privacy and data security governance are central challenges for smart cities, and smart city applications have been proven to contribute significantly to improving city security and transportation based on empirical analysis.
Rathee et al. (Rathee et al., 2022)	A trust-based mechanism for drones in smart cities	The blockchain-based trust formation scheme on ad hoc UAV networks can improve security, track malicious devices, and effectively maintain smart city communication performance.

Source: Database 2025

Table 6 shows that the main security and privacy challenges of smart cities lie in the vulnerability of massive and distributed IoT infrastructure. The study of (Sefati et al., 2024) shows that the integration of blockchain and federated learning within the framework of BFLIoT is able to improve the security, scalability, efficiency, and protection of IoT data privacy, while lowering the risk of data leakage and system latency. These findings show that privacy-preserving technology is no longer just an experimental option, but has evolved into a practical solution for urban

data management. From a policy perspective, these results indicate the need for regulatory instruments that encourage or require the adoption of privacy-enhancing technologies (PETs) such as federated learning, advanced encryption, and blockchain in smart city projects, especially in critical sectors such as transportation, energy, and digital public services.

In addition to IoT infrastructure, the security aspects of communications and unmanned aerial systems (UAVs) have also emerged as strategic issues in smart cities. Semenov et al. (Semenov et al., 2025) shows that the Fourier transformation-based steganography method is able to improve the data security of ADS-B UAVs, reduce signal distortion, and strengthen the resiliency of UAV communications to support sustainable smart city operations. Meanwhile, Rathee et al. (Rathee et al., 2022) emphasizes the importance of blockchain-based trust mechanisms on ad hoc UAV networks to track malicious devices and maintain communication performance. The policy implications of these two studies are related to technical standards and safety certification, namely the need to establish national or international standards regarding the security of UAV communications, the obligation to audit the security of urban drone systems, and the integration of security requirements in the procurement process of UAV technology by city governments.

The governance and regulatory dimensions are reinforced by Eskridge (Eskridge, 2019) and Naili et al. (2024), who highlight that privacy governance and regulatory compliance are key prerequisites for the success of smart cities. Eskridge (Eskridge, 2019) points out that privacy governance, data security, and surveillance should be positioned at the core of smart city architectures to mitigate the risk of data misuse and over-surveillance practices. Naili et al. (Naili et al., 2024) Add that while the legal framework has provided the basis for IoT-based health data protection, a more detailed technical regulation is still needed to ensure effective implementation. Therefore, relevant policy instruments include institutional coordination between data regulators, health authorities, and municipal governments, as well as public participation in the formulation of privacy policies so that the resulting policies are not only legalistic but also reflect societal expectations and values. Overall, this synthesis of five key articles reinforces the need for a multi-level policy framework that integrates regulations, technical standards, institutional governance, and citizen engagement in protecting the security and privacy of smart cities.

4. Discussion

From a digital communication governance perspective, the findings indicate that data protection in smart cities is not only a technical and

regulatory issue but also a communication process involving the production, transmission, and interpretation of data-related information. The dominance of technological themes such as IoT and artificial intelligence suggests that communication flows in smart city systems are increasingly mediated by data infrastructures, shaping how risks are perceived and how trust is constructed between institutions and citizens.

This finding is consistent with previous studies (Ahad et al., 2020; Allam & Dhunny, 2019; Bibri, 2018; Hashem et al., 2016), which highlight the central role of IoT and big data in smart city systems. However, unlike prior research that primarily focuses on technological efficiency, this study reveals that the dominance of these technologies also reflects underlying communication processes, particularly in how data is circulated and interpreted within governance systems.

The implementation of data protection and security policies in smart cities is increasingly challenged by the rapid expansion of the Internet of Things (IoT), big data, and artificial intelligence (AI), which continuously increase the scale, complexity, and sensitivity of urban data collection (Ahad et al., 2020; Allam & Dhunny, 2019; Bibri, 2018; Hashem et al., 2016). This technological growth creates a causal escalation: more connected systems generate more data, which in turn amplifies privacy risks and cybersecurity vulnerabilities, thereby requiring more adaptive and integrated governance responses. The persistence of privacy and security risks across different studies suggests that these challenges are structurally embedded within data-driven communication systems rather than being context-specific. The continuous expansion of data flows increases information asymmetry between institutions and citizens, thereby intensifying risk perception and reducing transparency.

The findings indicate that large volumes of personal and behavioral data generated by connected devices significantly increase the risks of data leakage, misuse, and unauthorized surveillance (A. Kumar et al., 2022; Mimo & McDaniel, 2022; Odeh et al., 2024). This result is consistent with previous studies, suggesting that data vulnerability is structurally embedded within smart city infrastructures rather than context-specific. The causal mechanism is clear: increased data flows without proportional governance capacity lead to systemic risks in data protection and citizen privacy.

These risks are further intensified by increasingly sophisticated cyber threats targeting interconnected infrastructures such as smart grids, transportation systems, and healthcare platforms (Mohamed et al., 2020; Naeem et al., 2025; Wu et al., 2020). However, existing approaches often address these risks in a fragmented manner, focusing either on technical

solutions or regulatory frameworks. This study contributes by demonstrating that such fragmentation limits policy effectiveness and that integrated governance approaches are required to address the complexity of smart city data ecosystems. Therefore, policy approaches must move beyond fragmented technical solutions and prioritize comprehensive data protection strategies that balance innovation with privacy and security requirements.

Evidence from high-impact studies demonstrates that privacy-preserving and decentralized technologies provide a strong operational foundation for data protection in smart cities. Technologies such as blockchain enhance data integrity and trust, while federated learning and differential privacy enable data analysis without exposing raw personal data. These findings confirm that technological innovation plays a critical role in mitigating privacy risks while maintaining data utility.

Consistent with previous research (Dagher et al., 2018; Hammi et al., 2018; Mezquita et al., 2023; Padma & Ramaiah, 2024)This study confirms that blockchain-based frameworks enhance authentication, access control, and data integrity. However, unlike earlier studies that focus primarily on technical efficiency, this research highlights that the effectiveness of these technologies depends on their integration with governance mechanisms. This finding extends existing literature by emphasizing that technological solutions alone are insufficient without institutional and regulatory alignment.

While federated learning and differential privacy enable data analytics without transferring raw personal data (Samanta & Sarkar, 2025; Sefati et al., 2024; Zhu et al., 2024)These technologies support the principle of privacy by design and align with emerging regulatory requirements such as GDPR compliance and consent management (Stefanouli & Economou, 2019), (Pina, 2023). From a practical perspective, these findings imply that policymakers should establish mandatory technical standards for IoT security, implement regular security audits, and require certification for privacy-enhancing technologies. Such measures ensure that technological innovation aligns with regulatory requirements and reduces systemic vulnerabilities. This study contributes by providing evidence-based justification for integrating emerging technologies into policy frameworks, thereby enhancing both operational effectiveness and regulatory compliance in smart city systems. (Vandercruysse et al., 2024).

Beyond technological safeguards, effective data protection requires coordinated institutional governance and citizen-centered policy frameworks. From a multi-level governance perspective, data protection involves interactions between municipal authorities, national regulators,

private sector actors, and civil society (Ha & Vu, 2024; Hong et al., 2022). The findings demonstrate that governance fragmentation across these actors reduces policy effectiveness and creates inconsistencies in implementation.

Consistent with previous studies (Eskridge, 2019; Mobilio, 2023)This research confirms that privacy governance and regulatory oversight must be embedded within smart city systems. However, unlike prior studies that focus primarily on legal frameworks, this study highlights the importance of institutional coordination and stakeholder collaboration. This difference arises from the integrative methodological approach used in this study, which combines bibliometric mapping with policy analysis to provide a more comprehensive understanding of governance challenges.

From a practical perspective, these findings suggest that governments should establish dedicated urban data governance units, strengthen inter-agency coordination, and promote public participation in data policy formulation. These measures ensure that data protection policies are not only legally compliant but also socially legitimate. This study contributes by providing a multi-actor governance model that addresses coordination challenges and enhances accountability in smart city ecosystems. (Ha & Vu, 2024; Hong et al., 2022). Public participation mechanisms should also be strengthened to ensure that data governance reflects societal values and expectations (Lnenicka et al., 2025). Taken together, these findings support a multi-level policy framework operating at city, national, and cross-border levels—that integrates regulatory instruments, technical standards, and institutional governance mechanisms to build trustworthy, resilient, and sustainable smart city ecosystems.

Building on these findings, this study proposes a multi-level policy framework consisting of three interconnected dimensions: regulatory instruments, technological safeguards, and institutional governance. The causal logic underlying this framework is as follows: technological expansion generates data risks, which require regulatory responses, supported by institutional coordination to ensure effective implementation. This integrative model provides a structured approach for aligning innovation with data protection objectives. First, regulatory instruments establish legal standards, including data protection laws, consent mechanisms, and compliance frameworks. Second, technological safeguards, such as blockchain, federated learning, and encryption, provide operational mechanisms to secure data. Third, institutional governance ensures coordination among stakeholders, including government agencies, private actors, and civil society.

This framework contributes theoretically by extending digital governance literature into a socio-technical and multi-level model of data protection. Practically, it provides actionable guidance for policymakers to design adaptive and integrated policies that balance innovation with privacy protection. By linking empirical findings with policy design, this study addresses the gap between knowledge production and governance implementation, offering a comprehensive and evidence-based approach to smart city data protection. From a practical perspective, these findings imply that policymakers should not only strengthen technical safeguards but also develop communication-based strategies, including transparent data policies, risk communication mechanisms, and citizen engagement platforms. Such approaches are essential to enhance public trust and ensure the legitimacy of data protection policies in smart city governance.

However, the expansion of data-driven technologies creates inherent tensions between innovation and privacy protection, requiring policymakers to balance efficiency and rights protection. This study suggests that future research should focus on empirical validation of the proposed framework in different governance contexts, particularly in developing countries. Such research is essential to assess the applicability and effectiveness of integrated data protection policies in diverse institutional environments. While smart city systems rely on extensive data collection to improve efficiency, excessive data use may lead to surveillance risks and erosion of public trust. Therefore, policymakers must balance these competing objectives by adopting adaptive regulatory frameworks that protect individual rights while enabling technological innovation. Ultimately, this study redefines data protection in smart cities as a communication-centered governance challenge, where trust, transparency, and citizen engagement are as critical as technological and regulatory solutions.

5. Conclusion

This study provides a comprehensive and integrative analysis of data protection and security in smart cities by combining bibliometric mapping with policy-oriented synthesis. The findings reveal a clear transformation in the research landscape, shifting from a predominantly technology-driven focus toward a governance-centered perspective. Data protection is no longer merely a technical issue related to cybersecurity or system design, but a complex socio-technical governance challenge involving the interaction of technological infrastructures, regulatory frameworks, and institutional arrangements. This study demonstrates that the increasing reliance on data-intensive technologies such as IoT and

artificial intelligence inherently generates new privacy and security risks, which require coordinated and adaptive governance responses.

From a theoretical perspective, this research advances digital governance and multi-level governance frameworks by conceptualizing data protection as a dynamic and integrated socio-technical system. Unlike previous studies that treat technological and regulatory dimensions as separate domains, this study demonstrates their interdependence through a causal mechanism in which technological expansion leads to increased data risks, necessitating regulatory intervention and institutional coordination. By introducing a policy-oriented bibliometric synthesis approach, this study contributes to bridging the gap between empirical knowledge production and governance design, offering a more structured and evidence-based understanding of data protection in smart city ecosystems.

From a practical and policy perspective, the study proposes a multi-level policy framework that integrates three key dimensions: regulatory instruments, technological safeguards, and institutional governance. The findings suggest that effective data protection requires not only the adoption of privacy-enhancing technologies such as blockchain, federated learning, and encryption, but also the establishment of coordinated governance mechanisms involving multiple stakeholders, including government agencies, private actors, and civil society. This integrative approach enables policymakers to balance technological innovation with the protection of citizen rights, thereby enhancing trust, accountability, and resilience in smart city systems.

Furthermore, this study contributes to the literature by demonstrating that privacy-enhancing technologies should be understood not merely as technical tools, but as governance instruments that shape accountability, transparency, and trust in digital environments. By linking technological innovation with governance mechanisms, this research provides a novel perspective that challenges the traditional separation between technology and policy. As such, it offers a more holistic and adaptive framework for understanding and addressing data protection challenges in increasingly complex and data-driven urban systems.

Despite its contributions, this study has several limitations. The analysis is limited to the Scopus database, which may exclude relevant grey literature such as policy reports and governmental documents. In addition, the reliance on bibliometric methods emphasizes patterns in academic publications and may not fully capture the complexities of policy implementation in real-world contexts. The proposed framework also requires empirical validation to assess its applicability across different

institutional and regional settings. These limitations suggest the need for further research that combines bibliometric analysis with qualitative and case-based approaches.

Future research should focus on validating the proposed framework through empirical case studies and comparative analysis across different governance contexts. In particular, studies examining how data protection policies are implemented in developing countries would provide valuable insights into institutional capacity, regulatory challenges, and contextual adaptation. Longitudinal research is also needed to understand how governance mechanisms evolve in response to rapid technological change. Ultimately, this study repositions data protection as a central pillar of smart city governance, emphasizing its critical role in ensuring sustainable, trustworthy, and citizen-centered digital transformation.

Reference

Ahad, M. A., Paiva, S., Tripathi, G., & Feroz, N. (2020). Enabling technologies and sustainable smart cities. *Sustainable Cities and Society*, *61*, 102301. https://doi.org/10.1016/j.scs.2020.102301

Allam, Z., & Dhunny, Z. A. (2019). On big data, artificial intelligence, and smart cities. *Cities*, *89*, 80–91. https://doi.org/10.1016/j.cities.2019.01.032

Allam, Z., Sharifi, A., Bibri, S. E., Jones, D. S., & Krogstie, J. (2022). The Metaverse as a Virtual Form of Smart Cities: Opportunities and Challenges for Environmental, Economic, and Social Sustainability in Urban Futures. *Smart Cities*, *5*(3), 771–801. https://doi.org/10.3390/smartcities5030040

Alshmrany, S. (2025). Securing smart cities: privacy-preserving IoT with optimized gated lounge attention dropout mechanism. *Neural Computing and Applications*, *37*(18), 12825–12850. https://doi.org/10.1007/s00521-025-11110-y

Angelini, M., Ciccotelli, C., Franchina, L., Marchetti-Spaccamela, A., & Querzoni, L. (2020). Italian National Framework for Cybersecurity and Data Protection. In A. L., N. M., I. G.F., R. K., & D. P. (Eds.), *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Vol. 12121 LNCS* (pp. 127–142). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-3-030-55196-4_8

Angus, A., Duan, Z., Zussman, G., & Kostic, Z. (2022). Real-Time Video

Anonymization in Smart City Intersections. *2022 IEEE 19th International Conference on Mobile Ad Hoc and Smart Systems (MASS)*, 514–522. https://doi.org/10.1109/MASS56207.2022.00078

Baas, J., Schotten, M., Plume, A., Côté, G., & Karimi, R. (2020). Scopus is a curated, high-quality bibliometric data source for academic research in quantitative science studies. *Quantitative Science Studies*, *1*(1), 377–386. https://doi.org/10.1162/qss_a_00019

Baran, B., Mamis, M. S., & Alagoz, B. B. (2016). Utilization of energy from waste potential in Turkey as a distributed secondary renewable energy source. *Renewable Energy*, *90*, 493–500. https://doi.org/10.1016/j.renene.2015.12.070

Bhardwaj, A., Kumar, M., Stephan, T., Shankar, A., Ghalib, M. R., & Abujar, S. (2022). IAF: IoT Attack Framework and Unique Taxonomy. *Journal of Circuits, Systems and Computers*, *31*(02). https://doi.org/10.1142/S0218126622500293

Bibri, S. E. (2018). The IoT for smart sustainable cities of the future: An analytical framework for sensor-based big data applications for environmental sustainability. *Sustainable Cities and Society*, *38*, 230–253. https://doi.org/10.1016/j.scs.2017.12.034

Blumenthal, M. S. (2021). Security done right can make smart cities wise. *Communications of the ACM*, *64*(9), 25–27. https://doi.org/10.1145/3473608

Chanduví, D. A. G., Lama, G. L. R., & Morey, N. D. (2015). Analysis of Research Literature of Professional Competency Models with a Cognitive-motivational Approach. *Procedia - Social and Behavioral Sciences*, *171*, 1400–1409. https://doi.org/10.1016/j.sbspro.2015.01.260

Chhabra, J., & Jaglan, A. (2024). Exploring the Land-Use Efficiency Dynamics and Improvement Potential in the Smart City Mission. In *Advances in 21st Century Human Settlements: Vol. Part F3155* (pp. 69–74). Springer. https://doi.org/10.1007/978-981-99-8811-2_6

Cortegiani, A., Ippolito, M., Ingoglia, G., Manca, A., Cugusi, L., Severin, A., Strinzel, M., Panzarella, V., Campisi, G., Manoj, L., Gregoretti, C., Einav, S., Moher, D., & Giarratano, A. (2020). Citations and metrics of journals discontinued from Scopus for publication concerns: the GhoS(t)copus Project. *F1000Research*, *9*, 415. https://doi.org/10.12688/f1000research.23847.2

Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable Cities and Society*, *39*, 283–297. https://doi.org/10.1016/j.scs.2018.02.014

Dincă, G., Milan, A. A., Andronic, M. L., Pasztori, A. M., & Dincă, D. (2022). Does the Circular Economy Contribute to Smart Cities' Sustainable Development? *International Journal of Environmental Research and Public Health*, *19*(13), 7627. https://doi.org/10.3390/ijerph19137627

Eskridge, M. (2019). Privacy and security data governance: surveillance mechanisms and resilience risks of smart city technologies. *Contemporary Readings in Law and Social Justice*, *11*(2), 63–69. https://doi.org/10.22381/CRLSJ11220199

Franke, J., & Gailhofer, P. (2021). Data Governance and Regulation for Sustainable Smart Cities. *Frontiers in Sustainable Cities*, *3*. https://doi.org/10.3389/frsc.2021.763788

Ha, H. T., & Vu, T. Van. (2024). POTENTIAL CONFLICTS IN PERSONAL DATA PROTECTION UNDER CURRENT LEGISLATION IN VIETNAM COMPARED WITH THE EUROPEAN GENERAL DATA PROTECTION REGULATION. *Access to Justice in Eastern Europe*, *7*(3), 505–526. https://doi.org/10.33327/AJEE-18-7.3-a000304

Haddaway, N. R., Page, M. J., Pritchard, C. C., & McGuinness, L. A. (2022). PRISMA2020: An R package and Shiny app for producing PRISMA 2020-compliant flow diagrams, with interactivity for optimized digital transparency and Open Synthesis. *Campbell Systematic Reviews*, *18*(2), e1230. https://doi.org/10.1002/cl2.1230

Hammi, M. T., Hammi, B., Bellot, P., & Serhrouchni, A. (2018). Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. *Computers and Security*, *78*, 126–142. https://doi.org/10.1016/j.cose.2018.06.004

Hashem, I. A. T., Chang, V., Anuar, N. B., Adewole, K., Yaqoob, I., Gani, A., Ahmed, E., & Chiroma, H. (2016). The role of big data in smart cities. *International Journal of Information Management*, *36*(5), 748–758. https://doi.org/10.1016/j.ijinfomgt.2016.05.002

Hong, Y. M., Zhang, M., & Liu, Y. (2022). Promoting Safe and Orderly

Flow of Cross-border Data to Lead Development of Globalization of Digital Economy. *Bulletin of Chinese Academy of Sciences*, *37*(10). https://doi.org/10.16418/j.issn.1000-3045.20220802002

Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2024). Understanding Local Government Cybersecurity Policy: A Concept Map and Framework. *Information*, *15*(6), 342. https://doi.org/10.3390/info15060342

Hughes-Noehrer, L., Aubert Bonn, N., De Maria, M., Evans, T. R., Farran, E. K., Fortunato, L., Henderson, E. L., Jacobs, N., Munafò, M. R., Stewart, S. L. K., & Stewart, A. J. (2024). UK Reproducibility Network open and transparent research practices survey dataset. *Scientific Data* , *11*(1), 912. https://doi.org/10.1038/s41597-024-03786-z

Jat, M. K., & Saxena, A. (2018). Sustainable Urban Growth using Geoinformatics and CA based Modelling. *Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance*, 499–508. https://doi.org/10.1145/3209415.3209429

Javed, A. R., Shahzad, F., ur Rehman, S., Zikria, Y. Bin, Razzak, I., Jalil, Z., & Xu, G. (2022). Future smart cities: Requirements, emerging technologies, applications, challenges, and future aspects. *Cities*, *129*, 103794.

Jin, Y., & Wang, Y. (2025). Reassessing smart city development and personal data protection: A regulatory framework. *International Review of Economics & Finance*, *99*, 104022. https://doi.org/10.1016/j.iref.2025.104022

Khan, A. A., Laghari, A. A., Alroobaea, R., Baqasah, A. M., Alsafyani, M., Bacarra, R., & Alsayaydeh, J. A. J. (2024). Secure Remote Sensing Data With Blockchain Distributed Ledger Technology: A Solution for Smart Cities. *IEEE Access*, *12*, 69383–69396. https://doi.org/10.1109/ACCESS.2024.3401591

Kumar, A., Upadhyay, A., Mishra, N., Nath, S., Yadav, K. R., & Sharma, G. (2022). Privacy and Security Concerns in Edge Computing-Based Smart Cities. In *Studies in Computational Intelligence* (Vol. 1030, pp. 89–110). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-3-030-96737-6_5

Kumar, K. S., Prabakaran, D., Kumaran, R. S., & Yamuna, I. (2022). Privacy and security of smart systems. In *Intelligent Green Technologies*

for Sustainable Smart Cities (pp. 291–315). Wiley. https://doi.org/10.1002/9781119816096.ch14

Kumar, P., Kumar, R., Srivastava, G., Gupta, G. P., Tripathi, R., Gadekallu, T. R., & Xiong, N. N. (2021). PPSF: A Privacy-Preserving and Secure Framework Using Blockchain-Based Machine-Learning for IoT-Driven Smart Cities. *IEEE Transactions on Network Science and Engineering*, *8*(3), 2326–2341. https://doi.org/10.1109/TNSE.2021.3089435

Lawelai, H. (2023). Understanding Digital Governance in Smart Cities: In-Depth Study Utilizing VOSviewer and CiteSpace. *E3S Web of Conferences*, *440*, 07003. https://doi.org/10.1051/e3sconf/202344007003

Li, B., Yang, X., & Wu, X. (2024). Role of net-zero renewable-based transportation systems in smart cities toward enhancing cultural diversity: Realistic model in digital twin. *Sustainable Energy Technologies and Assessments*, *65*, 103715. https://doi.org/10.1016/j.seta.2024.103715

Lnenicka, M., Kysela, T., & Horák, O. (2025). Building security and resilience: a guide to implementing effective cybersecurity and data protection measures in smart cities. *Smart and Sustainable Built Environment*. https://doi.org/10.1108/SASBE-09-2024-0363

Lv, Z., Li, X., Wang, W., Zhang, B., Hu, J., & Feng, S. (2018). Government affairs service platform for smart city. *Future Generation Computer Systems*, *81*, 443–451. https://doi.org/10.1016/j.future.2017.08.047

Medková, J. (2024). Classification of Datasets Used in Data Anonymization for IoT Environment. In F. H., C. R., H.-M. A., & A. M. (Eds.), *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Vol. 14748 LNAI* (pp. 80–92). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-981-97-4677-4_8

Mezquita, Y., Gil-González, A. B., Prieto, J., & Corchado, J. M. (2023). Blockchain Technology-Based Smart Cities: A Privacy-Preservation Review. In *Advances in Information Security* (Vol. 102, pp. 109–124). Springer. https://doi.org/10.1007/978-3-031-25506-9_6

Mimo, E. M., & McDaniel, T. (2022). Smart Cities: A Survey of Tech-Induced Privacy Concerns. In *Advanced Sciences and Technologies for*

Security Applications (pp. 1–22). Springer. https://doi.org/10.1007/978-3-031-04424-3_1

Mishra, K. N., & Chakraborty, C. (2020). A Novel Approach Toward Enhancing the Quality of Life in Smart Cities Using Clouds and IoT-Based Technologies. In *Internet of Things* (pp. 19–35). Springer International Publishing. https://doi.org/10.1007/978-3-030-18732-3_2

Mobilio, G. (2023). Your face is not new to me – Regulating the surveillance power of facial recognition technologies. *Internet Policy Review*, *12*(1), 1–31. https://doi.org/10.14763/2023.1.1699

Mohamed, N., Al-Jaroodi, J., Jawhar, I., & Kesserwan, N. (2020). Data-Driven Security for Smart City Systems: Carving a Trail. *IEEE Access*, *8*, 147211–147230. https://doi.org/10.1109/ACCESS.2020.3015510

Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2010). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *International Journal of Surgery*, *8*(5), 336–341. https://doi.org/10.1016/j.ijsu.2010.02.007

Mondschein, J., Clark-Ginsberg, A., & Kuehn, A. (2021). Smart cities as large technological systems: Overcoming organizational challenges in smart cities through collective action. *Sustainable Cities and Society*, *67*, 102730. https://doi.org/10.1016/j.scs.2021.102730

Moustafa, N. (2021). A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets. *Sustainable Cities and Society*, *72*. https://doi.org/10.1016/j.scs.2021.102994

Naeem, H., Ullah, F., & Srivastava, G. (2025). Classification of intrusion cyber-attacks in smart power grids using deep ensemble learning with metaheuristic-based optimization. *Expert Systems*, *42*(1). https://doi.org/10.1111/exsy.13556

Naili, Y. T., Afrilies, M. H., Garunja, E., & Purwono, P. (2024). Protection of patient data privacy on IoT devices for healthcare in the era of smart cities: a health law perspective. *Jurnal Hukum Novelty*, *15*(1), 87–105. https://doi.org/10.26555/novelty.v15i1.a28457

Nef, T., Urwyler, P., Büchler, M., Tarnanas, I., Stucki, R., Cazzoli, D., Müri, R., & Mosimann, U. (2015). Evaluation of Three State-of-the-Art Classifiers for Recognition of Activities of Daily Living from

Smart Home Ambient Data. *Sensors*, *15*(5), 11725–11740. https://doi.org/10.3390/s150511725

Odeh, A., Taleb, A. A., Alhajahjeh, T., Aparicio, F., Hamed, S., Daradkeh, N. Al, & Al-Jarallah, N. A. (2024). Data privacy and compliance in IoT. In *Smart and Agile Cybersecurity for IoT and IIoT Environments* (pp. 128–144). IGI Global. https://doi.org/10.4018/979-8-3693-3431-7.ch006

Ogunkan, D. V., & Ogunkan, S. K. (2025). Exploring big data applications in sustainable urban infrastructure: A review. *Urban Governance*, *5*(1), 54–68. https://doi.org/10.1016/j.ugj.2025.02.003

Padma, A., & Ramaiah, M. (2024). Blockchain Based an Efficient and Secure Privacy Preserved Framework for Smart Cities. *IEEE Access*, *12*, 21985–22002. https://doi.org/10.1109/ACCESS.2024.3364078

Padrão, P., Ribeiro, M. I., & Lopes, I. (2024). Implementation of the General Regulation on Data Protection – In the Intermunicipal Community of Douro, Portugal. In M. C., R. A., & C. L. J.M. (Eds.), *Lecture Notes in Networks and Systems* (Vol. 773, pp. 360–367). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-3-031-44131-8_35

Papaiakovou, A., Nika, C., & Vergados, D. D. (2022). E-Privacy Issues in the Smart Cities Environment. *2022 13th International Conference on Information, Intelligence, Systems & Applications (IISA)*, 1–7. https://doi.org/10.1109/IISA56318.2022.9904395

Pina, P. (2023). Adoption of GDPR for Personal Data Protection in Smart Cities. In *Protecting User Privacy in Web Search Utilization* (pp. 251–268). IGI Global. https://doi.org/10.4018/978-1-6684-6914-9.ch013

Priya Dharshini, K., Gopalakrishnan, D., Shankar, C. K., & Ramya, R. (2022). A Survey on IoT Applications in Smart Cities. In *EAI/Springer Innovations in Communication and Computing* (pp. 179–204). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-3-030-66607-1_9

Rathee, G., Kumar, A., Kerrache, C. A., & Iqbal, R. (2022). A trust-based mechanism for drones in smart cities. *IET Smart Cities*, *4*(4), 255–264. https://doi.org/10.1049/smc2.12039

Raza, A., Badidi, E., Hayajneh, M., Barka, E., & Harrouss, O. El. (2024). Blockchain-Based Reputation and Trust Management for Smart Grids, Healthcare, and Transportation: A Review. *IEEE Access*, *12*,

196887–196913. https://doi.org/10.1109/ACCESS.2024.3521428

Roldan, L. R., Trujillo, A. E., Miyatake, M. N., & Chano, J. (2019). Color Watermarking based on DCT and YCbCr Color Space for Privacy Preservation in Smart Cities. *Proceedings of the 2019 3rd International Conference on Digital Signal Processing*, *Part F1479*, 119–123. https://doi.org/10.1145/3316551.3316556

Samanta, S., & Sarkar, A. (2025). Blockchain integrated DFL model for IIoT data security in smart cities. *International Journal of Information Technology (Singapore)*, *17*(2), 911–923. https://doi.org/10.1007/s41870-024-02354-3

Sánchez Alcón, J., López, L., Martínez, J.-F., & Rubio Cifuentes, G. (2015). Trust and Privacy Solutions Based on Holistic Service Requirements. *Sensors*, *16*(1), 16. https://doi.org/10.3390/s16010016

Sayah, Z., Kazar, O., Lejdel, B., Laouid, A., & Ghenabzia, A. (2021). An intelligent system for energy management in smart cities based on big data and ontology. *Smart and Sustainable Built Environment*, *10*(2), 169–192. https://doi.org/10.1108/SASBE-07-2019-0087

Sefati, S. S., Craciunescu, R., Arasteh, B., Halunga, S., Fratu, O., & Tal, I. (2024). Cybersecurity in a Scalable Smart City Framework Using Blockchain and Federated Learning for Internet of Things (IoT). *Smart Cities*, *7*(5), 2802–2841. https://doi.org/10.3390/smartcities7050109

Semenov, S., Krupska-Klimczak, M., Mazurek, P., Zhang, M., & Chernykh, O. (2025). Improving Unmanned Aerial Vehicle Security as a Factor in Sustainable Development of Smart City Infrastructure: Automatic Dependent Surveillance–Broadcast (ADS-B) Data Protection. *Sustainability (Switzerland)*, *17*(4). https://doi.org/10.3390/su17041553

Shafik, W., Kalinaki, K., & Zakari, R. Y. (2024). Blockchain's Motivation for IoT-Enabled Smart City. In *Secure and Intelligent IoT-Enabled Smart Cities* (pp. 195–221). IGI Global. https://doi.org/10.4018/979-8-3693-2373-1.ch010

Sharma, S., & Mishra, N. (2024). Analyzing the Potential of Smart Cities: Technologies, Frameworks, Vulnerabilities, Threats, and Information Security Solutions. *2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS)*, 1570–1574. https://doi.org/10.1109/ICETSIS61505.2024.10459607

Singh, S., Sharma, P. K., Yoon, B., Shojafar, M., Cho, G. H., & Ra, I.-H. (2020). Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city. *Sustainable Cities and Society*, *63*. https://doi.org/10.1016/j.scs.2020.102364

Somanathan Pillai, S. E. V., Vallabhaneni, R., Vaddadi, S. A., Addula, S. R., & Ananthan, B. (2025). Archimedes assisted LSTM model for blockchain based privacy preserving IoT with smart cities. *Indonesian Journal of Electrical Engineering and Computer Science*, *37*(1), 488. https://doi.org/10.11591/ijeecs.v37.i1.pp488-497

Srivastava, R., & Sharifi, A. (2022). Smart Cities: Concepts and Underlying Principles. In *Urban Book Series* (pp. 39–65). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-3-030-95037-8_3

Stefanouli, M., & Economou, C. (2019). Data Protection in Smart Cities: Application of the EU GDPR. In N. E.G. & K. I.D. (Eds.), *Advances in Intelligent Systems and Computing* (Vol. 879, pp. 748–755). Springer Verlag. https://doi.org/10.1007/978-3-030-02305-8_90

Sui, P., Li, X., & Bai, Y. (2017). A Study of Enhancing Privacy for Intelligent Transportation Systems: k -Correlation Privacy Model Against Moving Preference Attacks for Location Trajectory Data. *IEEE Access*, *5*, 24555–24567. https://doi.org/10.1109/ACCESS.2017.2767641

Sun, L., & Wu, S. (2020). Smart City Privacy Protection in Big Data Environment. In A. M., Y. N., & X. Z. (Eds.), *Advances in Intelligent Systems and Computing: Vol. 1117 AISC* (pp. 663–670). Springer. https://doi.org/10.1007/978-981-15-2568-1_91

Torre, D., Soltana, G., Sabetzadeh, M., Briand, L. C., Auffinger, Y., & Goes, P. (2019). Using Models to Enable Compliance Checking Against the GDPR: An Experience Report. In K. M., Y. T., Y. T., P. A., V. S., B. L., & B. L. (Eds.), *2019 ACM/IEEE 22nd International Conference on Model Driven Engineering Languages and Systems (MODELS)* (pp. 1–11). IEEE. https://doi.org/10.1109/MODELS.2019.00-20

V, L. K., M, M., Sheeba, A., & Subasini, C. . (2024). Cross Border Secure Messaging with Blockchain A Global Perspective. *2024 International Conference on Advances in Data Engineering and Intelligent Computing Systems (ADICS)*, 1–5.

https://doi.org/10.1109/ADICS58448.2024.10533628

Vandercruysse, L., Dooms, M., & Buts, C. (2024). Public procurement of smart city services: an exploration of data protection related ex ante transaction costs. *Digital Policy, Regulation and Governance*, *26*(6), 617–639. https://doi.org/10.1108/DPRG-11-2023-0159

Vashishth, T. K., Sharma, V., Sharma, K. K., Kumar, B., Chaudhary, S., & Panwar, R. (2024). Blockchain-Enabled Data Security and Integrity in IoT-Big Data Systems for Smart Cities. In *Internet of Things and Big Data Analytics-Based Manufacturing* (pp. 69–90). CRC Press. https://doi.org/10.1201/9781032673479-5

Verma, G., Gope, P., Saxena, N., & Kumar, N. (2022). CB-DA: Lightweight and Escrow-Free Certificate-Based Data Aggregation for Smart Grid. *IEEE Transactions on Dependable and Secure Computing*, *20*(3), 1–1. https://doi.org/10.1109/TDSC.2022.3169952

Vimercati, S. D. C. di, Foresti, S., Livraga, G., & Samarati, P. (2022). Digital infrastructure policies for data security and privacy in smart cities. In *Smart Cities Policies and Financing: Approaches and Solutions* (pp. 249–261). Elsevier. https://doi.org/10.1016/B978-0-12-819130-9.00007-3

Wang, Q., & Liu, Y. (2024). Beautifying urban environment: Smart city construction and sustainable pollution control in China. *Journal of Environmental Management*, *371*, 123262. https://doi.org/10.1016/j.jenvman.2024.123262

Wang, Y., & Kong, T. (2019). Air Quality Predictive Modeling Based on an Improved Decision Tree in a Weather-Smart Grid. *IEEE Access*, *7*, 172892–172901. https://doi.org/10.1109/ACCESS.2019.2956599

Wu, F., Li, X., Xu, L., Kumari, S., Lin, D., & Rodrigues, J. J. P. C. (2020). An anonymous and identity-trackable data transmission scheme for smart grid under smart city notion. *Annales Des Telecommunications/Annals of Telecommunications*, *75*(7–8), 307–317. https://doi.org/10.1007/s12243-020-00765-4

Xia, L., Semirumi, D. T., & Rezaei, R. (2023). A thorough examination of smart city applications: Exploring challenges and solutions throughout the life cycle with emphasis on safeguarding citizen privacy. *Sustainable Cities and Society*, *98*, 104771. https://doi.org/10.1016/j.scs.2023.104771

Xu, Z., Shao, T., Dong, Z., & Li, S. (2022). Research progress of heavy

metals in desert—visual analysis based on CiteSpace. *Environmental Science and Pollution Research*, *29*(29), 43648–43661. https://doi.org/10.1007/s11356-022-20216-y

Yan, Y., & Kunhui, Y. (2024). Novel cyber-physical architecture for optimal operation of renewable-based smart city considering false data injection attacks: Digital twin technologies for smart city infrastructure management. *Sustainable Energy Technologies and Assessments*, *65*, 103733. https://doi.org/10.1016/j.seta.2024.103733

Yang, Y., Kang, C., Gou, G., Li, Z., & Xiong, G. (2018). TLS/SSL Encrypted Traffic Classification with Autoencoder and Convolutional Neural Network. *2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, 362–369. https://doi.org/10.1109/HPCC/SmartCity/DSS.2018.00079

Yang, Z., Li, L., Yuan, H., Dong, Y., Liu, K., Lan, L., Lin, W., Jin, K., Zhu, C., Chai, C., Zhou, Q., Yan, Z., Dong, T., Zhou, L., & Fang, Y. (2020). Evaluation of Smart Energy Management Systems and Novel UV-Oriented Solution for Integration, Resilience, Inclusiveness and Sustainability. *2020 5th International Conference on Universal Village (UV)*, 1–49. https://doi.org/10.1109/UV50937.2020.9426217

Zhang, L., Ren, J., Yuan, H., Yang, Z., Wang, W., Guo, M., Cheng, G., Zhou, L., Tao, S., Zhang, L., Cui, H., & Fang, Y. (2020). Evaluation of Smart Healthcare Systems and Novel UV-Oriented Solution for Integration, Resilience, Inclusiveness and Sustainability. *2020 5th International Conference on Universal Village (UV)*, 1–28. https://doi.org/10.1109/UV50937.2020.9426210

Zhu, C., Zhu, X., & Qin, T. (2024). An Efficient Privacy Protection Mechanism for Blockchain-Based Federated Learning System in UAV-MEC Networks. *Sensors*, *24*(5), 1364. https://doi.org/10.3390/s24051364