

Strategic Insights and Trends in Population Data Security for Urban Demography in Smart Cities

Herman Lawelai¹, Eko Priyo Purnomo^{2*}, Achmad Nurmandi², Hazel Jovita³, and Elaine M. Baulete³

¹ Department of Government Studies, Faculty of Social Sciences and Political Sciences, Universitas Muhammadiyah Buton, Indonesia

² Department of Government Affairs and Administration, Jusuf Kalla School of Government, Universitas Muhammadiyah Yogyakarta, Indonesia

³ Department of Political Science, College of Arts and Social Sciences, Mindanao State University-Iligan Institute of Technology, Philippines

* Eko Priyo Purnomo, corresponding author. Email: eko@umy.ac.id

Submitted: 19 December 2024. Accepted: 30 November 2025. Published: 1 July 2026

Volume 35, 2027. pp. 511–532. <http://doi.org/10.25133/JPSSv352027.026>

Abstract

This study examines how scholarship on population data security has evolved within urban demography and smart city research. Using a scientometric and bibliometric design, the study analyzed Scopus-indexed publications from 2014 to 2023 with RStudio/Bibliometrix and CiteSpace to map publication growth, international collaboration, keyword trends, citation bursts, conceptual clusters, and thematic evolution. The findings show rapid publication growth, with a marked increase in 2023, and identify China, India, and the United States as major collaboration hubs. Topic mapping indicates a shift from general smart city and Internet of Things security concerns toward blockchain, machine learning, privacy by design, advanced analytics, and decentralized data governance. The conceptual structure reveals three interconnected knowledge clusters: information security governance, technical cybersecurity implementation, and urban infrastructure management. This study contributes to population and social studies by clarifying how data protection, demographic governance, and digital urban infrastructure intersect in smart city development. Rather than proposing a new framework, it synthesizes the intellectual structure of the field and offers evidence-based insights for strengthening privacy protection, institutional coordination, and adaptive cybersecurity governance in future smart cities.

Keywords

Blockchain technology; cybersecurity; digital privacy; population data security; smart cities

Introduction

Amid rapid urban transformation, smart cities have become a prominent model for integrating advanced technology into public administration (Yigitcanlar, 2015), improving service efficiency, sustainability, and quality of life (Ainane et al., 2018, 2019; Liu & Wu, 2023; Xihua & Goyal, 2022). Urban governments increasingly use digital tools and interconnected systems to manage services, optimize resources, and strengthen citizen engagement (Kourtiti et al., 2017). At the center of this transformation is public administration data, which supports planning, infrastructure management, and evidence-based decision-making (Jyothi et al., 2024). As smart cities expand, the security of population data becomes central to the reliability of urban governance.

As cities become more dependent on digital integration, safeguarding sensitive information becomes essential to public trust (Sidorenko et al., 2019). The interconnectivity of smart city systems creates a broad attack surface for cyber threats, making data security a core concern for urban governance (Demertzi et al., 2023). Protecting public administration data also sustains the continuity of smart city services and the legitimacy of digital government (Suresh Kumar et al., 2022). Data security is therefore not only a technical matter. It is also an institutional challenge that requires coordination among agencies, technology providers, regulatory bodies, and citizens.

Despite the efficiency gains offered by smart city technologies, serious data security challenges continue to threaten the integrity and confidentiality of public administration information (Ismagilova et al., 2022). Interconnected urban systems intensify vulnerabilities by linking sensors, platforms, databases, and service networks that are exposed to cyberattacks and unauthorized access (Kitchin & Dodge, 2019). These risks are reinforced by rapid technological change, which often develops faster than security policy, regulatory capacity, and institutional preparedness (Verma et al., 2022). The resulting problem involves systemic risk, interoperability, accountability, and ethical data handling.

Existing literature on data security in smart cities frequently examines separate dimensions of the problem, including specific security technologies, privacy standards, or policy frameworks (Blumenthal, 2021; De Capitani di Vimercati et al., 2022; Kasar & Kshirsagar, 2021; Wu et al., 2020). However, these studies remain fragmented across cybersecurity, urban governance, and information systems research. This fragmentation limits understanding of how population data security should be governed in complex urban environments. A consolidated bibliometric and scientometric synthesis is therefore needed to identify the intellectual structure of the field, clarify theoretical connections, and reveal strategic research gaps.

To address this gap, this study employs scientometric and bibliometric analysis to map the development of scholarship on population data security in smart cities. RStudio/Bibliometrix was used to examine conceptual structures and topic evolution, while CiteSpace was used to detect citation bursts, co-citation patterns, and timeline clusters. These tools were selected because they support both quantitative mapping and interpretive analysis of large bibliographic datasets. The approach enables the study to identify dominant contributors, evolving research themes, and strategic knowledge frontiers in population data security.

The rationale for this study lies in the growing urgency of strengthening data security in smart city governance (De Capitani di Vimercati et al., 2022). Public administration data are increasingly exposed to sophisticated digital threats, including unauthorized access, cyberattacks, and misuse of personal information (Gázquez, 2021; Wirtz & Weyerer, 2017). By systematically analyzing publication trends and thematic structures, this study evaluates how scholarship has addressed these challenges and identifies policy-oriented directions for future urban governance. The analysis also situates population data security within broader debates on privacy, trust, and demographic governance in digitally mediated cities.

The main objective of this study is to provide a comprehensive analysis of public administration data security in smart cities using advanced visual analytic tools. The study addresses five research questions: (1) How has the number of related publications developed, and what patterns of international collaboration are visible? (2) What trends and strategic issues shape public administration data security in smart cities? (3) What conceptual structures and topic clusters define this research field? (4) How have major topics evolved across the 2014–2023 period? (5) What strategic insights support stronger future security policies?

This study contributes to smart city and population studies by linking data protection, urban demography, and digital governance. Its contribution lies not only in mapping publication patterns but also in synthesizing fragmented literature into an integrated sociotechnical perspective that connects technological systems, governance arrangements, and ethical concerns. The findings provide policymakers, urban planners, and technology developers with evidence-based insights into current security challenges and strategic responses. In doing so, the study supports safer, more trusted, and more resilient smart city environments.

Theoretical framework

Smart cities and urban governance

Smart cities are increasingly understood as urban ecosystems that integrate information and communication technologies to improve sustainability, service efficiency, and citizen well-being (Jebbar et al., 2024; Subrahmanyam, 2025). They rely on the Internet of Things (IoT), artificial intelligence (AI), and big data to optimize infrastructure in transportation, healthcare, energy, and public services (Hossain & Hasan, 2025; Humayun et al., 2019). Urban governance theory emphasizes transparency, accountability, and trust as key conditions for effective digital transformation (Almulhim & Yigitcanlar, 2025; Bozkurt et al., 2025). These principles become more urgent as smart cities generate and process large volumes of population data.

Smart city governance requires alignment among technological innovation, public trust, and regulatory compliance. Digital governance frameworks provide mechanisms for managing security, privacy, interoperability, and accountability (Anvari et al., 2023; Humayun et al., 2019). Technological advancement alone does not secure urban systems without institutional capacity, clear rules, and coordinated implementation (Čolić et al., 2020; Jarour & Mocanu, 2025). This study therefore positions population data security as a sociotechnical issue in which political, institutional, technological, and citizen dimensions operate together.

Cybersecurity, blockchain, and artificial intelligence

Cybersecurity challenges in smart cities arise from dependence on IoT, big data, and distributed digital infrastructure, which expose urban systems to breaches, malware, denial-of-service attacks, and unauthorized access (Anajemba et al., 2025; Hossain & Hasan, 2025). Protective measures such as encryption, authentication, monitoring, and incident response are essential for securing public data (Barletta et al., 2024; Ravikumar et al., 2024). Blockchain technology is widely discussed because its decentralized and tamper-resistant architecture can strengthen transparency, traceability, and data integrity (Ahmad et al., 2021; Krishnan & Ganesan, 2021; Xagoraris et al., 2024).

AI and machine learning (ML) also contribute to cybersecurity through real-time threat detection, anomaly identification, predictive modeling, and automated response mechanisms (Barletta et al., 2024; Hossain & Hasan, 2025). Recent studies show that AI-driven systems can strengthen the monitoring of sophisticated cyber threats in smart cities (Hamid & Bawany, 2024; Ravikumar et al., 2024). At the same time, blockchain-enabled models support privacy-preserving data sharing and decentralized storage (Ahmad et al., 2021; Krishnan & Ganesan, 2021). Together, AI and blockchain support adaptive security architectures that protect both urban infrastructure and citizens' data.

Digital transformation, risk governance, and data ethics

Digital transformation in smart cities reflects the integration of ICT into governance systems to improve service delivery, transparency, and citizen participation (Alkubaisi & Abdallah, 2024; Jarour & Mocanu, 2025). This transition requires adaptive governance mechanisms that respond to rapid technological change while controlling vulnerabilities. Studies emphasize that international collaboration is essential for developing cybersecurity policies that transcend national boundaries (Barletta et al., 2024; Čolić et al., 2020). Such collaboration strengthens interoperability standards and improves resilience against transnational cyber threats.

The ethical dimensions of population data security are equally important. Privacy, surveillance, and social control raise questions about the legitimacy of smart city projects and the rights of citizens whose data are collected and processed (Foth et al., 2021; Hardi et al., 2025; Raghav et al., 2025). The literature emphasizes privacy by design, in which security and privacy protections are embedded from the earliest stages of system development (Hamid & Bawany, 2024; Ravikumar et al., 2024; Subrahmanyam, 2025). Risk governance in smart cities must therefore combine technical defenses with ethical safeguards that support inclusive, transparent, and equitable urban development (Aslam et al., 2022; Benedik & Al-Khateeb, 2021).

Methodology

This study employed scientometric and bibliometric analysis to examine research on public administration data security in smart cities. This design was selected because it enables systematic mapping of knowledge domains, thematic clusters, collaboration networks, and topic evolution. The Scopus database was used because it provides broad coverage of peer-reviewed literature across the social sciences, information systems, public administration, and

technology (Schotten et al., 2017; Zhu & Liu, 2020). The analysis focused on identifying publication trends, conceptual structures, and the development of research topics related to population data security, urban demography, and smart city governance.

The Scopus database was searched to collect relevant bibliographic records, and the dataset was exported in CSV format for analysis. The data were imported into RStudio using the Bibliometrix package and into CiteSpace for visualization and science mapping. RStudio/Bibliometrix supported descriptive bibliometric analysis, co-word analysis, conceptual structure mapping, and topic evolution. CiteSpace supported burst detection, co-citation analysis, and timeline visualization. The combined use of these tools strengthened analytical reliability and enabled both quantitative synthesis and qualitative interpretation of the research field (Guo et al., 2023).

Protocol and framework

This study followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines to document the identification, screening, eligibility, and inclusion stages of the bibliographic dataset. PRISMA provides a transparent structure for reporting search procedures and selection criteria (Wang et al., 2019). In this study, PRISMA was adapted for scientometric mapping rather than for a conventional systematic review. This adaptation is appropriate because the study classifies, visualizes, and interprets the overall knowledge structure of a research domain (Petersen et al., 2008).

Inclusion and exclusion criteria

After the search phase, the identified records were screened to remove irrelevant documents. The retrieved studies were assessed against predefined inclusion and exclusion criteria to ensure alignment with the research questions. This process retained a significant but manageable body of literature that reflects recent developments in population data security, urban demography, and cybersecurity in smart cities. The search was limited to publications from January 1, 2014, to December 31, 2023, to capture contemporary digital security challenges and avoid historical bias in the analysis.

The inclusion criteria were as follows:

- Language: Only English-language studies were included to ensure accessibility and compatibility with bibliometric and scientometric analysis.
- Publication type: Journal articles, conference proceedings, and book series were included when they presented complete research outputs and met peer-review standards.
- Relevance to the research questions: Studies were included when they directly addressed population data security, digital privacy, risk mitigation, cybersecurity infrastructure, and their applications in smart cities or urban demography.
- Publication version: When multiple versions of a study were available, the most recent and complete version was selected to ensure current data and analysis.

The following publication types were excluded from further review:

- Studies not written in English.

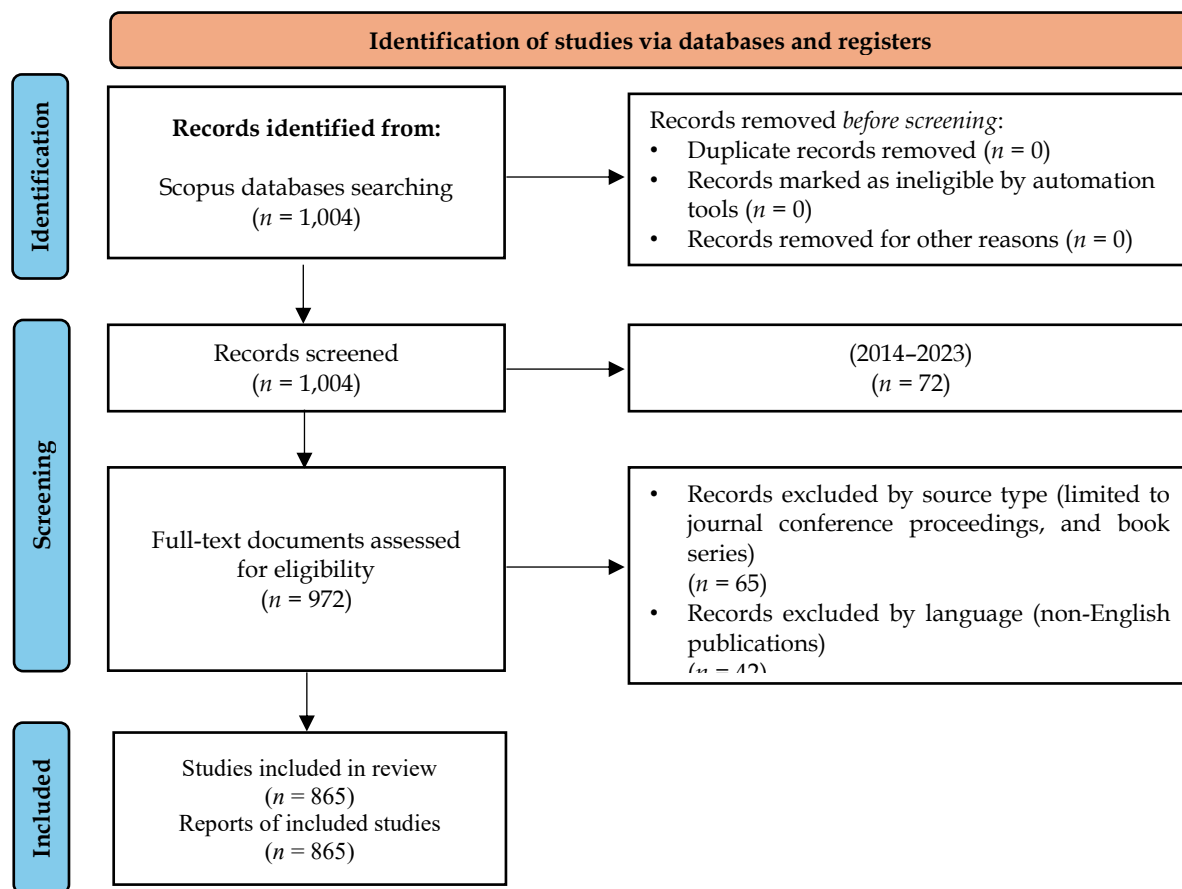
- Papers that provided only general policy recommendations without empirical analysis, data, or methodological contributions were excluded.
- Editorials, books, and book chapters that did not follow a standardized peer-review process.
- Workshop presentations, symposium summaries, and non-peer-reviewed materials.
- Articles lacking adequate methodology, including unclear data sources, unclear analysis techniques, or no validation of results.
- Short documents with fewer than five pages were excluded because they often lack sufficient detail for scientometric analysis.
- Studies for which the full text was unavailable were excluded because they prevented thorough examination and verification.

Search strategy and data processing

The search was conducted on October 3, 2024, using the following refined query:

TITLE-ABS-KEY (("population data security" OR "data protection" OR "digital privacy" OR "cybersecurity") AND ("smart cities" OR "urban demography" OR "urban governance"))

This refinement avoided overly broad terms such as "population safety," which could retrieve documents outside the intended cybersecurity and data governance scope. The initial search yielded 1,044 documents for screening. After publication year, source type, and language filters were applied in accordance with the PRISMA protocol, 865 publications were retained for analysis. Data processing followed three analytical stages: identification, screening, and inclusion. Figure 1 illustrates the selection and refinement process for publications on population data security in urban demography within smart cities.

Figure 1: Modified PRISMA Diagram Illustrating the Article Selection Process in a Systematic Review

Note: Adapted from Wang et al. (2019)

In the screening stage, 72 documents were excluded because they fell outside the 2014–2023 publication period. The remaining 972 records were assessed for eligibility. The eligibility stage applied source-type restrictions to journals, conference proceedings, and book series, excluding 65 documents. Non-English publications were then excluded, removing 42 records. This process produced a final dataset of 865 publications for scientometric and bibliometric analysis.

Validation as a study strength

A key strength of this study is its validation process. Cross-validation was conducted between RStudio/Bibliometrix and CiteSpace outputs to ensure consistency across analytical tools. Keywords, citation metadata, and source information were checked to reduce database-related inconsistencies. This multi-platform procedure strengthens the robustness of the scientometric workflow and increases confidence in the findings.

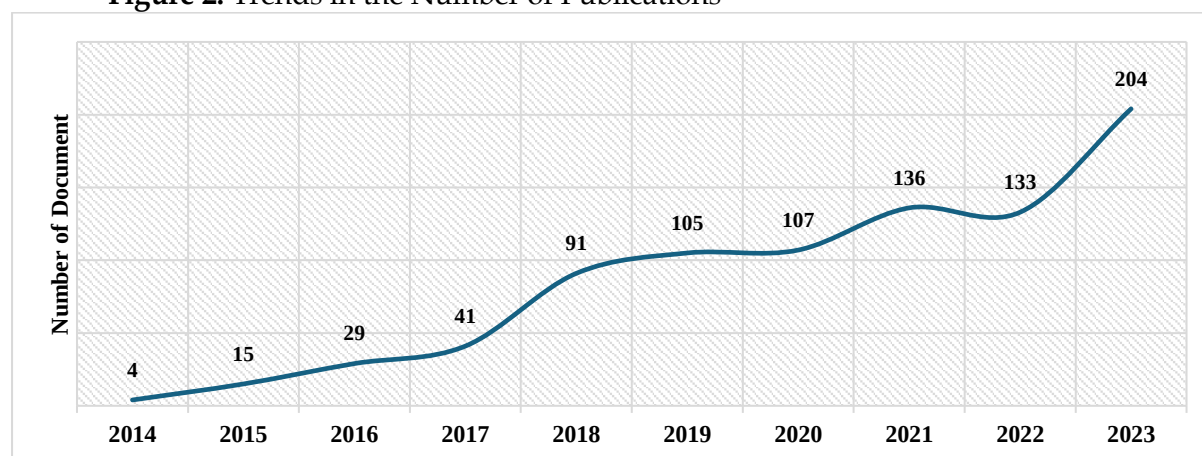
Results and discussion

Publication volume and collaboration map

Publication trends and collaboration networks provide important indicators for understanding the development of research on public administration data security in smart cities. Publication growth reflects increasing scholarly attention, whereas collaboration patterns show the extent of international research cooperation and knowledge exchange within the field.

Figure 2 illustrates publication trends on public administration data security in smart cities from 2014 to 2023. In 2014, there were only four publications; however, the number increased to 41 by 2017 and reached 136 in 2021. Although a slight decline occurred in 2022 (133 publications), output rose markedly in 2023 (204 publications). This pattern demonstrates growing academic and policy interest in data security within smart city development over the past decade.

Figure 2: Trends in the Number of Publications

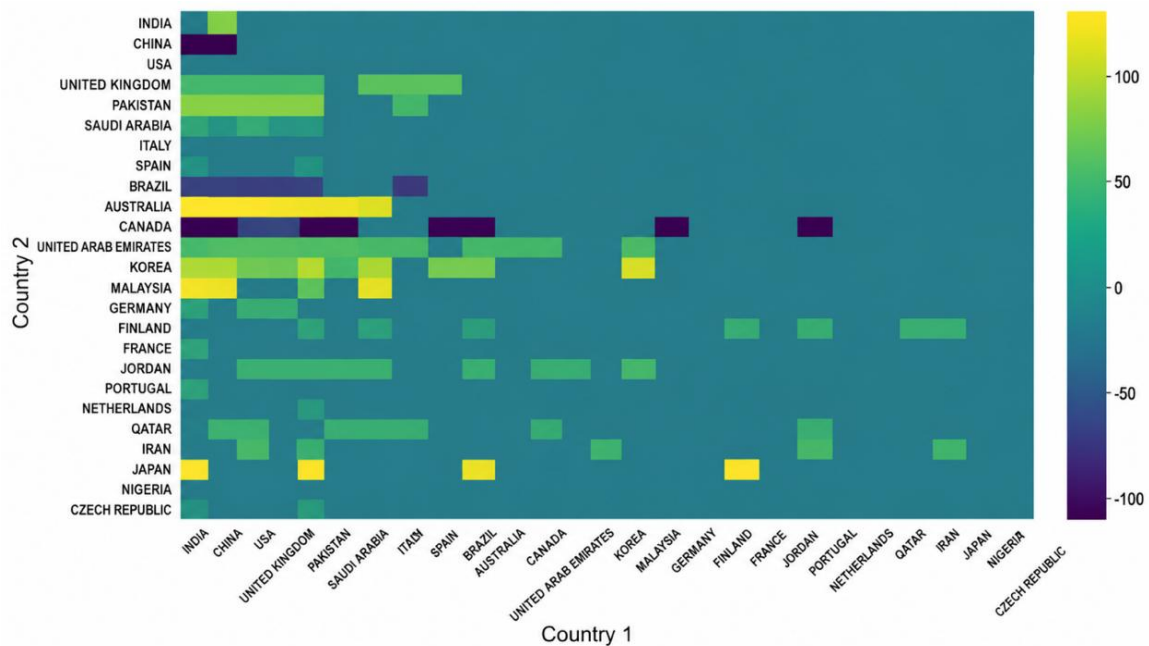


Note: Data processed from the Scopus database

The increase in publication output corresponds with the expansion of digital governance policies and cybersecurity regulations in urban environments. For example, the implementation of the General Data Protection Regulation (GDPR) in the European Union encouraged research on the applicability of comparable policies in smart cities (Edwards, 2016; Vitunskaitė et al., 2019). At the same time, blockchain, IoT, and AI became central research themes because of their relevance to urban data security and governance capacity.

Figure 3 illustrates international collaboration networks in research on public administration data security in smart cities. Connections between countries indicate co-authorship intensity, and line thickness reflects the strength of collaboration. China, India, and the United States appear as dominant contributors and major collaboration hubs within the global research network.

Figure 3: Collaboration Intensity Heatmap Based on Co-Authorship Across the Top 25 Countries



Note: Authors' elaboration using RStudio and Scopus data

The collaboration pattern in Figure 3 indicates that data security in smart cities is a transnational research issue that requires cross-border cooperation and interdisciplinary knowledge exchange. International collaboration supports the development of interoperability standards, cybersecurity strategies, and governance frameworks (Lawelai et al., 2025; Melaku, 2023). It also facilitates the exchange of technological expertise and joint innovation in addressing complex urban security challenges.

Public administration data security trends and issues in smart cities

Scientometric trend analysis identifies dominant themes, emerging technologies, and evolving research priorities related to public administration data security in smart cities. This analysis clarifies how scholarly attention has shifted in response to technological development, cybersecurity risk, and policy concern.

Figure 4 presents the most frequently occurring keywords in research on smart cities and public administration data security. Keywords such as "smart city," "Internet of Things," and "network security" are the most prominent, indicating that these topics form the core of the literature. The prominence of these keywords reflects the increasing integration of IoT, big data, and blockchain technologies into smart city governance systems (Alsammak et al., 2022; Rajalakshmi et al., 2023). These technologies improve administrative efficiency and urban connectivity, yet they also introduce risks related to privacy, cybersecurity, and data governance. Blockchain has received attention because it can reduce data manipulation and improve transparency in digital governance systems (Iqbal & Matulevičius, 2019). Big data analytics also supports evidence-based decision-making in smart cities (Jayanthi & Pravallika Reddy, 2020).

Figure 4: Word Cloud Topic of Public Administration Data Security in Smart Cities



Note: Authors' elaboration using RStudio and Scopus data

The findings in Figure 4 show that current research increasingly emphasizes the balance between technological innovation and data protection. Secure smart city systems require both technical advancement and governance mechanisms that address privacy, accountability, and institutional coordination.

Table 1 shows the temporal distribution of major research topics between 2019 and 2023. “Smart City” is the most frequent topic, with 180 occurrences, followed by “Security,” “Blockchain,” and “Machine Learning.”

Table 1: Topic Trends in Public Administration Data Security in Smart Cities

Topic	Freq	Year Q1	Year Med	Year Q3
Smart City	180	2019	2021	2022
Security	90	2019	2021	2022
Blockchain	49	2020	2022	2023
Machine Learning	42	2022	2022	2023
IoT	36	2019	2022	2023
Big Data	28	2018	2020	2022
Cloud Computing	25	2019	2019	2022
Innovation	17	2019	2020	2021
Cryptography	10	2019	2020	2023
Safety	10	2022	2023	2023

Note: Authors' elaboration using RStudio and Scopus data; Freq (frequency) indicates the number of publications associated with each topic; Year Q1 (first quartile), Year Med (median), and Year Q3 (third quartile publication years) represent the temporal distribution of topic emergence within the dataset.

Topics such as “Cryptography” and “Safety” appear less frequently despite their relevance to cybersecurity research. The temporal pattern shown in Table 1 demonstrates a gradual shift

from general smart city discussions toward more specialized themes related to AI-driven security, blockchain systems, and advanced data management technologies. The increasing prominence of blockchain, machine learning, and IoT after 2020 indicates growing academic interest in decentralized and intelligent security systems (Ahmed et al., 2022). Likewise, the emergence of “Big Data” and “Cloud Computing” reflects the increasing complexity of data governance and digital infrastructure management in smart city environments (Kushwaha, 2023).

Table 2 identifies the topics with the strongest citation bursts between 2014 and 2023. Topics related to the Internet of Things (IoT) and data communication systems demonstrated the highest citation intensity, indicating sustained scholarly attention during the observation period.

Table 2: Top Topics with the Strongest Citation Bursts

Keywords	Strength	Begin	End	2014–2023
Internet of Things (IoT)	5.23	2015	2020	
Ubiquitous Computing	7.02	2018	2019	
Trusted Computing	5.14	2018	2019	
Monitoring	3.99	2018	2019	
Data Communication Systems	9.77	2019	2020	
Privacy by Design	6.06	2020	2021	
Security of Data	5.52	2020	2021	
Advanced Analytics	4.44	2020	2021	
Technological Innovation	4.22	2021	2023	
Digital Transformation	3.84	2021	2023	

Note: Authors' elaboration using CiteSpace and Scopus data; The red bars indicate periods of statistically significant citation bursts based on CiteSpace burst detection. The turquoise bars denote the full observation window (2014–2023). Thus, the red portion highlights intervals of elevated scholarly attention, whereas the turquoise portion provides the temporal boundary for the analysis.

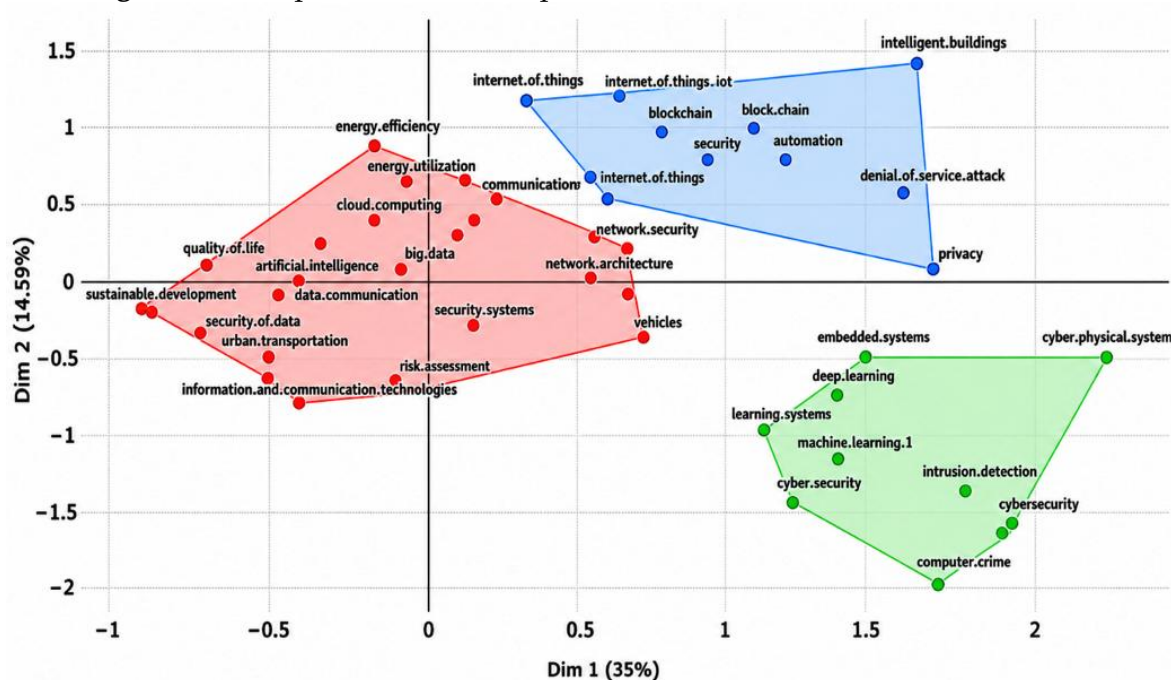
The increasing citation intensity of IoT-related studies between 2015 and 2020 reflects the rapid adoption of interconnected devices in urban infrastructure systems. Similarly, the strong citation burst for data communication systems between 2019 and 2020 highlights the growing importance of secure communication architectures in smart city governance. Other topics, including ubiquitous computing, privacy by design, and advanced analytics, also experienced substantial citation growth. This pattern indicates a transition from infrastructure-focused discussions toward integrated approaches emphasizing privacy, ethics, and intelligent data governance.

The increasing attention to “Privacy by Design” and “Security of Data” since 2020 reflects stronger awareness of the ethical implications of smart city governance (Carullo & Ernst, 2020; Jaakonmäki et al., 2020). Smart city systems collect and process large volumes of personal data, making privacy protection a central concern. Recent studies therefore emphasize embedding privacy and security protections into system design from the earliest stages of technological development (Salnitri et al., 2020).

Conceptual structure and topic mapping

Conceptual structure mapping was used to identify thematic relationships and intellectual structures within the literature on public administration data security in smart cities. Figure 5 illustrates conceptual relationships among key themes in smart city data security research. The visualization identifies three major clusters represented by red, blue, and green groupings. The red cluster focuses on foundational information security concepts, including network security, information governance, and data protection (Awad, 2018). The blue cluster emphasizes technical implementation issues such as IoT systems, wireless communication, and cybersecurity threats (Awad, 2018). The green cluster covers broader urban management themes, including urban mobility, energy management, and critical infrastructure systems (Ngossaha et al., 2018).

Figure 5: Conceptual Structure Map



Note: Authors' elaboration using RStudio and Scopus data; The colors indicate the conceptual clusters identified through the co-occurrence analysis. Red represents foundational information security concepts, blue represents technical and implementation-level concepts, and green represents broader urban management and infrastructure concepts. The axes (Dim 1 and Dim 2) reflect the principal coordinates derived from the conceptual structure analysis.

The conceptual clustering in Figure 5 shows that population data security in smart cities extends beyond technical cybersecurity. It reflects interaction among governance structures, digital infrastructure, and urban management systems. The findings support the view that smart city data security should be approached as a multidimensional sociotechnical issue.

Timeline and topic evolution of public administration data security

Timeline analysis was conducted to examine the evolution of research themes and identify major shifts in scholarly attention between 2014 and 2023. Table 3 illustrates the evolution of major research clusters identified using CiteSpace. The results show that energy management, big data, intelligent transportation systems, blockchain, and artificial intelligence emerged as

dominant research areas during the observation period. Early research between 2014 and 2017 focused primarily on IoT systems, cloud computing, and cyber-physical infrastructure.

Table 3: Timeline View: Topic of Public Administration Data Security in Smart Cities

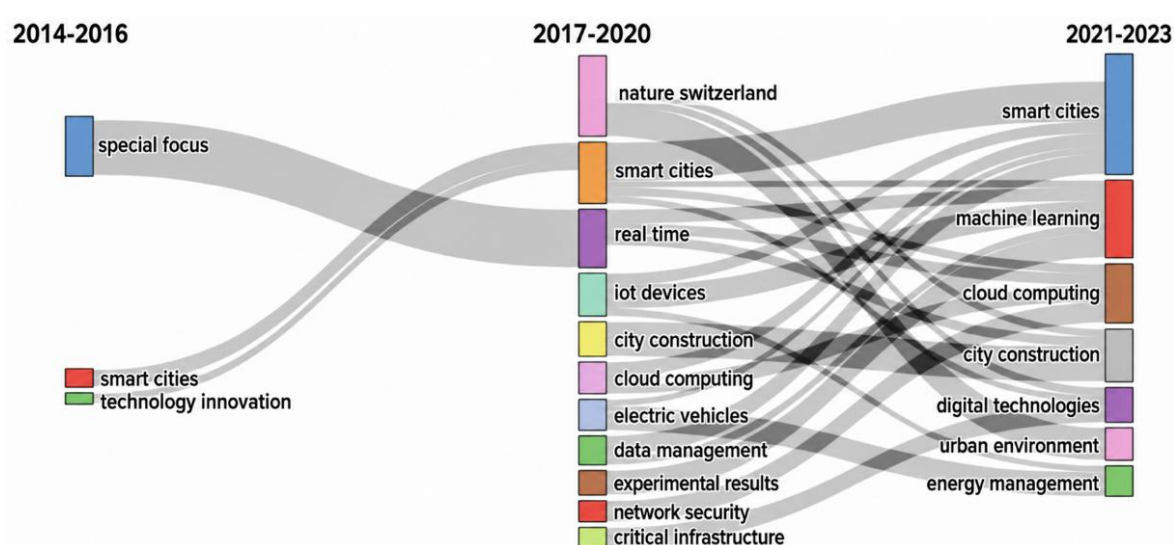
Cluster	Size	Silhouette	Label (LLR)	Keywords and Frequency	Year
0	41	0.699	energy management (173.8, 1.0E-4)	58 security systems, 49 machine learning, 48 deep learning, 40 energy efficiency, 37 embedded systems.	2019
1	36	0.798	big data (300.09, 1.0E-4)	467 smart city, 261 internet of things, 182 network security, 80 internet of things (IoT), 68 big data.	2017
2	22	0.621	intelligent transportation system (121.27, 1.0E-4)	22 urban transportation, 15 intelligent transportation systems, 14 intelligent vehicle highway systems, 14 vehicles	2021
3	29	0.666	unmanned aerial vehicles application (155.58, 1.0E-4)	44 data privacy, 28 internet of things (IoT), 25 5g mobile communication systems, 22 intrusion detection, 16 risk assessment.	2019
4	31	0.779	case study (208.89, 1.0E-4)	127 smart cities, 65 cyber security, 53 sustainable development, 36 security of data, 30 information and communication technology.	2018
5	26	0.648	using blockchain technology (258.04, 1.0E-4)	64 blockchain, 63 security, 41 cryptography, 41 cybersecurity, 40 blockchain.	2019
6	27	0.728	artificial intelligence (205.81, 1.0E-4)	47 artificial intelligence, 42 urban growth, 32 decision making, 16 public administration, 14 game theory.	2018
7	16	0.785	to-centralized smart technology management (162.22, 1.0E-4)	57 automation, 30 intelligent buildings, 27 network architecture, 18 denial of service attack, 12 application programs.	2020
8	11	0.872	federated capability-based access control mechanism (129.01, 1.0E-4)	20 edge computing, 15 green computing, 12 fog computing, 7 smartphones, 6 smart contracts.	2020
9	8	0.881	smart connected buildings design automation (100.01, 1.0E-4)	13 optimization, 5 environmental impact, 5 genetic algorithms, 5 traffic congestion, 4 algorithms.	2017
10	11	0.935	lcl filter (118.18, 1.0E-4)	16 cyberattacks, 15 energy security, 6 federated learning, 5 electric vehicles, 4 charging (batteries).	2019

Note: Authors' elaboration using CiteSpace and Scopus data

More recent studies emphasize blockchain technology, AI-driven security systems, and decentralized governance models (Balcerzak et al., 2022). The emergence of topics such as federated access control, edge computing, and smart contracts after 2020 indicates a shift toward decentralized and adaptive security architectures. This evolution reflects broader changes in smart city governance, where cybersecurity is increasingly integrated with intelligent infrastructure management and real-time data processing.

Figure 6 shows the longitudinal evolution of research topics between 2014 and 2023. The visualization shows how early research themes developed into more specialized and technologically sophisticated topics over time. Between 2014 and 2016, research focused mainly on technological innovation and smart city infrastructure development (Angelidou, 2015; Meijer & Bolívar, 2016).

Figure 6: Topic Evolution of Public Administration Data Security in Smart Cities



Note: Authors' elaboration using RStudio and Scopus data

Between 2017 and 2020, scholarly attention shifted toward cloud computing, IoT devices, data management, and network security (Chaudhary et al., 2017). This transition reflects the growing need to manage increasing volumes of urban data while addressing cybersecurity vulnerabilities. Between 2021 and 2023, more advanced themes emerged, including machine learning, digital technologies, and energy management (Androniceanu, 2023). This evolution indicates that smart city data security research has moved from foundational infrastructure concerns toward integrated governance, intelligent systems, and adaptive cybersecurity frameworks.

Strategic insights for population data security in future smart cities

Strategic insights into population data security in future smart cities should focus on integrating advanced technologies with robust governance frameworks. As cities increasingly rely on interconnected systems, blockchain, AI, and IoT are important for managing large-scale data networks (Banciu et al., 2020; Ilyas, 2021; Yemanov et al., 2023). Blockchain enhances transparency and security through decentralized data management, reducing risks of manipulation and unauthorized access. AI strengthens predictive capabilities for identifying

threats before escalation. These technologies must operate within legal, institutional, and ethical frameworks that protect data and respect citizens' privacy and autonomy.

Another important finding concerns the growing need for cross-border collaboration and policy standardization to address increasingly complex global cyber threats. Smart cities frequently face transnational cybersecurity challenges because urban data flows are increasingly interconnected across countries and institutions (Almeida, 2023). The collaboration analysis demonstrates that China, India, and the United States currently dominate research production and international cooperation in this field. Nevertheless, broader international partnerships remain necessary to support policy harmonization and interoperability standards in smart city governance. Research on GDPR implementation further demonstrates how regulatory frameworks can stimulate academic development and policy innovation. Consequently, future regulations related to smart city data governance may play a critical role in encouraging more secure and coordinated cybersecurity practices at both local and global levels.

Ensuring sustainable and secure data management in smart cities requires adaptive governance strategies that respond to technological innovation (Anthony Jnr, 2025). As smart city infrastructure becomes more sophisticated, policies governing data security must also evolve (Fernandez-Monge et al., 2024; Kontogeorgis & Varotsis, 2021). Flexible governance mechanisms are important because AI, IoT, and big data generate innovation while also creating new vulnerabilities (Linkov et al., 2014). Future policies should prioritize proactive approaches that integrate data protection into the earliest stages of urban planning and technological design.

Theoretical implications

These findings show that the growth of research and international collaboration on population data security in smart cities underscores the importance of governance capacity, rather than technology alone, in strengthening urban resilience. Technological innovation cannot ensure effective cybersecurity without institutional support and adaptive governance mechanisms. This finding is consistent with studies that highlight transparency and accountability as core dimensions of smart city governance (Almulhim & Yigitcanlar, 2025; Meijer & Bolívar, 2016). It also shows that Asian countries, particularly China and India, increasingly shape collaboration and policy-oriented research agendas in this field.

The emergence of blockchain, IoT, and privacy-by-design themes in keyword evolution and citation bursts reflects a paradigm shift toward sociotechnical integration in smart city governance. Previous studies similarly emphasize embedding privacy and security protections directly into system design (Ahmad et al., 2021; Salnitri et al., 2020). IoT is also recognized as both an opportunity and a vulnerability within smart city ecosystems (Prakoso et al., 2023). The present findings extend this work by showing how privacy, decentralization, and intelligent security systems are becoming interconnected research priorities.

The conceptual structure analysis identified three interconnected clusters: governance and policy, technological systems, and urban infrastructure management. This structure indicates that smart city data security should be understood as an interdependent sociotechnical system rather than as a set of isolated technical components. Earlier studies focused mainly on infrastructure-related vulnerabilities (Ngossaha et al., 2018). The present findings extend this perspective by demonstrating the overlap among governance, infrastructure, and

technological mechanisms. In this regard, blockchain-enabled decentralized governance models offer alternatives to conventional centralized systems (Balcerzak et al., 2022).

The timeline analysis between 2014 and 2023 demonstrates a transition from early discussions centered on cloud computing and IoT toward advanced themes involving blockchain, AI, and ethical governance. Similar trends appear in earlier studies emphasizing the foundational role of IoT and cloud infrastructure in smart city development (Angelidou, 2015; Chaudhary et al., 2017). The present findings differ by showing that decentralized and adaptive governance models are becoming central theoretical approaches for understanding population data security in smart city environments.

Practical implications

From a practical perspective, the findings show that technological security systems and smart city governance frameworks must adapt to increasingly complex and transnational cyber threats. Previous studies highlight the importance of infrastructure policy and cross-border collaboration in addressing cybersecurity challenges (Almeida, 2023; De Capitani di Vimercati et al., 2022). The present findings reinforce arguments for adaptive risk governance in managing emerging technological threats (Linkov et al., 2014). The dominance of Asian countries in research collaboration also indicates the growing importance of globally inclusive governance approaches beyond traditional Eurocentric perspectives.

The identified priority themes, namely AI, blockchain, and privacy by design, have direct implications for policymakers and practitioners. Previous studies advocate citizen-centered governance frameworks and adaptive governance in smart urban systems (Anthony Jnr, 2025; Fernandez-Monge et al., 2024). The present findings challenge perspectives that treat technical solutions as sufficient for smart city security (Blumenthal, 2021). Effective cybersecurity in smart cities requires sociotechnical integration involving governance, ethics, institutional trust, and technological innovation.

Consequently, ethical safeguards and adaptive governance mechanisms should be integrated alongside technological advancement to support secure urban planning and sustainable digital transformation. The results also clarify the strengths and limitations of current smart city security approaches, offering guidance for future policy development and implementation.

Strengths and limitations

The strength of this study lies in its combined use of performance analysis, science mapping, and topic evolution analysis to examine population data security in smart cities. Drawing on Scopus data and using both RStudio/Bibliometrix and CiteSpace, the study provides a transparent and reproducible overview of publication growth, collaboration patterns, conceptual clusters, and emerging research fronts. This design offers a strong empirical foundation for policy-oriented and theory-driven work on data governance in smart city environments.

The study is limited by its reliance on the Scopus database, English-language publications, and a defined 2014-2023 observation period. These criteria strengthen consistency but exclude relevant studies indexed in other databases, published in other languages, or appearing

outside the selected timeframe. Bibliometric and scientometric methods also provide macro-level patterns rather than detailed qualitative assessment of each study. Future research should combine bibliometric mapping with systematic content analysis, case studies, and comparative policy research across diverse urban contexts.

Conclusion

This study provides a comprehensive scientometric and bibliometric analysis of population data security in smart cities by examining publication trends, collaboration networks, conceptual structures, citation bursts, and thematic evolution between 2014 and 2023. The findings reveal a clear shift from technical and infrastructure-centered discussions toward integrated sociotechnical frameworks that combine governance, technology, and ethical safeguards. They also show that publication growth, international collaboration, blockchain, IoT, AI, and privacy by design are central to the current research agenda.

Future research should move beyond descriptive mapping by examining institutional, political, and ethical barriers to implementation across diverse urban contexts. Advancing this field requires closer integration between technological innovation and governance strategies that are inclusive, flexible, and rights-oriented. Smart cities can achieve sustainability and resilience when technological infrastructure is aligned with governance systems that protect citizens' rights, strengthen public trust, and ensure responsible use of population data.

Ethical consideration

Ethical approval was not required for this scientometric and bibliometric study because it analyzed published literature indexed in the Scopus database and did not involve human participants, identifiable personal data, or intervention procedures.

References

- Ahmad, I., Ashar, S. W., Khalid, U., Irfan, A., & Khalil, W. (2021). Blockchain for sustainable smart cities. In A. Solanki, A. Kumar, & A. Nayyar (Eds.), *Digital cities roadmap: IoT-based architecture and sustainable buildings* (pp. 127–161). Wiley. <https://doi.org/10.1002/9781119792079.ch4>
- Ahmed, I., Zhang, Y., Jeon, G., Lin, W., Khosravi, M. R., & Qi, L. (2022). A blockchain- and artificial intelligence-enabled smart IoT framework for sustainable city. *International Journal of Intelligent Systems*, 37(9), 6493–6507. <https://doi.org/10.1002/int.22852>
- Ainane, N., Ouzzif, M., & Bouragba, K. (2018). Data security of smart cities. In M. Ben Ahmed, A. A. Boudhir, & A. Younes (Eds.), *Proceedings of the 3rd International Conference on Smart City Applications* (Article 89, pp. 1–13). Association for Computing Machinery. <https://doi.org/10.1145/3286606.3286866>
- Ainane, N., Ouzzif, M., & Bouragba, K. (2019). Data security of smart cities. In M. Ben Ahmed, A. Boudhir, & A. Younes (Eds.), *Innovations in smart cities applications edition 2: SCA 2018 (Lecture notes in intelligent transportation and infrastructure)* (pp. 702–712). Springer. https://doi.org/10.1007/978-3-030-11196-0_58
- Alkubaisi, A., & Abdallah, W. (2024). Using information and communication technology for smart urban governance mediated by community engagement. In N. Mansour & L. M. Bujosa Vadell (Eds.), *Finance and law in the metaverse world (Contributions to finance and accounting)* (pp. 473–

- 484). Springer. https://doi.org/10.1007/978-3-031-67547-8_40
- Almeida, F. (2023). Prospects of cybersecurity in smart cities. *Future Internet*, 15(9), Article 285. <https://doi.org/10.3390/fi15090285>
- Almulhim, A. I., & Yigitcanlar, T. (2025). Understanding smart governance of sustainable cities: A review and multidimensional framework. *Smart Cities*, 8(4), Article 113. <https://doi.org/10.3390/smartcities8040113>
- Alsammak, I. L. H., Alomari, M. F., Nasir, I. S., & Itwee, W. H. (2022). A model for blockchain-based privacy-preserving for big data users on the internet of thing. *Indonesian Journal of Electrical Engineering and Computer Science*, 26(2), 974–988. <https://doi.org/10.11591/ijeecs.v26.i2.pp974-988>
- Anajemba, F. C., Anajemba, J. H., & Iwendi, C. (2025). Analyzing strategies for ensuring robust information security management in a smart city. In C. Iwendi, Z. Boulouard, & N. Kryvinska (Eds.), *Proceedings of the 4th International Conference on Advances in Communication Technology and Computer Engineering (ICACTCE'24): ICACTCE 2024 (Lecture notes in networks and systems, Vol. 1312)* (pp. 47–56). Springer. https://doi.org/10.1007/978-3-031-94620-2_5
- Androniceanu, A. (2023). The new trends of digital transformation and artificial intelligence in public administration. *Administratie si Management Public*, 2023(40), 147–155. <https://doi.org/10.24818/amp/2023.40-09>
- Angelidou, M. (2015). Smart cities: A conjuncture of four forces. *Cities*, 47, 95–106. <https://doi.org/10.1016/j.cities.2015.05.004>
- Anthony Jnr, B. (2025). Sustainable mobility governance in smart cities for urban policy development: A scoping review and conceptual model. *Smart and Sustainable Built Environment*, 14(3), 649–671. <https://doi.org/10.1108/SASBE-05-2023-0109>
- Anvari, R., Kumpikaite-Valiunienė, V., & Janjaria, M. (2023). Determinants of digital governance in the development of smart cities. In *2023 IEEE European Technology and Engineering Management Summit (E-TEMS)* (pp. 107–110). IEEE. <https://doi.org/10.1109/E-TEMS57541.2023.10424645>
- Aslam, M., Khan Abbasi, M. A., Khalid, T., Shan, R. U., Ullah, S., Ahmad, T., Saeed, S., Alabbad, D. A., & Ahmad, R. (2022). Getting smarter about smart cities: Improving data security and privacy through compliance. *Sensors*, 22(23), Article 9338. <https://doi.org/10.3390/s22239338>
- Awad, A. I. (2018). Introduction to information security foundations and applications. In *Information Security: Foundations, Technologies and Applications* (pp. 3–11). Institution of Engineering and Technology. https://doi.org/10.1049/PBSE001E_ch1
- Balcerzak, A. P., Nica, E., Rogalska, E., Poliak, M., Klieštík, T., & Sabie, O.-M. (2022). Blockchain technology and smart contracts in decentralized governance systems. *Administrative Sciences*, 12(3), Article 96. <https://doi.org/10.3390/admsci12030096>
- Banciu, D., Rădoi, M., & Belloiu, S. (2020). Information security awareness in Romanian public administration: An exploratory case study. *Studies in Informatics and Control*, 29(1), 121–129. <https://doi.org/10.24846/v29i1y202012>
- Barletta, V. S., Caivano, D., De Vincentiis, M., Pal, A., & Scalera, M. (2024). Hybrid quantum architecture for smart city security. *Journal of Systems and Software*, 217, Article 112161. <https://doi.org/10.1016/j.jss.2024.112161>
- Benedik, R., & Al-Khateeb, H. (2021). Digital citizens in a smart city: The impact and security challenges of IoT on citizen's data privacy. In R. Montasari, H. Jahankhani, & H. Al-Khateeb (Eds.), *Challenges in the IoT and smart environments (Advanced sciences and technologies for security applications)* (pp. 93–122). Springer. https://doi.org/10.1007/978-3-030-87166-6_5
- 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>
- Bozkurt, Y., Rossmann, A., Pervez, Z., & Ramzan, N. (2025). Assessing data governance models for smart cities: Benchmarking data governance models on the basis of European urban requirements. *Sustainable Cities and Society*, 130, Article 106528. <https://doi.org/10.1016/j.scs.2025.106528>
- Carullo, G., & Ernst, C. (2020). Data storage by public administrations. *European Public Law*, 26(3), 545–568. <https://doi.org/10.54648/euro2020055>
- Chaudhary, R., Kumar, N., & Zeadally, S. (2017). Network service chaining in fog and cloud computing for the 5G environment: Data management and security challenges. *IEEE Communications Magazine*, 55(11), 114–122. <https://doi.org/10.1109/MCOM.2017.1700102>

- Čolić, N., Manić, B., Niković, A., & Brankov, B. (2020). Grasping the framework for the urban governance of smart cities in Serbia: The case of INTERREG SMF project CLEVER. *Spatium*, (43), 26–34. <https://doi.org/10.2298/SPAT2043026C>
- De Capitani di Vimercati, S., Foresti, S., Livraga, G., & Samarati, P. (2022). Digital infrastructure policies for data security and privacy in smart cities. In J. R. Vacca (Ed.), *Smart cities policies and financing: Approaches and solutions* (pp. 249–261). Elsevier. <https://doi.org/10.1016/B978-0-12-819130-9.00007-3>
- Demertzi, V., Demertzis, S., & Demertzis, K. (2023). An overview of cyber threats, attacks and countermeasures on the primary domains of smart cities. *Applied Sciences*, 13(2), Article 790. <https://doi.org/10.3390/app13020790>
- Edwards, L. (2016). Privacy, security and data protection in smart cities: A Critical EU Law Perspective. *European Data Protection Law Review*, 2(1), 28–58. <https://doi.org/10.21552/EDPL/2016/1/6>
- Fernandez-Monge, F., Barns, S., Kattel, R., & Bria, F. (2024). Reclaiming data for improved city governance: Barcelona's New Data Deal. *Urban Studies*, 61(7), 1291–1307. <https://doi.org/10.1177/00420980231204835>
- Foth, M., Anastasiu, I., Mann, M., & Mitchell, P. (2021). From automation to autonomy: Technological sovereignty for better data care in smart cities. In B. T. Wang & C. M. Wang (Eds.), *Automating cities (Advances in 21st century human settlements)* (pp. 319–343). Springer. https://doi.org/10.1007/978-981-15-8670-5_13
- Gázquez, A. E. (2021). Ciberataque al SEPE: ¿posible responsabilidad patrimonial? [Cyber-attack on SEPE's service: Possible patrimonial liability?]. *Revista General de Derecho Administrativo*, 58, 1–26. https://www.iustel.com/v2/revistas/detalle_revista.asp?id_noticia=424244
- Guo, Y., Cai, S., Deng, J., Li, J., Qiu, L., Sun, Q., Cui, Y., Li, L., Yu, L., Yin, H., Sun, Z., & Zuo, L. (2023). Trends and hotspots of acupuncture for allergic rhinitis: A bibliometric analysis from 2002 to 2022. *Complementary Therapies in Medicine*, 78, Article 102984. <https://doi.org/10.1016/j.ctim.2023.102984>
- Hamid, S., & Bawany, N. Z. (2024). Federated learning for enhanced intrusion detection in smart city environments. In *2024 18th International Conference on Open Source Systems and Technologies (ICOSST)* (pp. 1–6). IEEE. <https://doi.org/10.1109/ICOSST64562.2024.10871154>
- Hardi, R., Nurmandi, A., Purwaningsih, T., & Manaf, H. A. (2025). Smart city governance and interoperability: Enhancing human security in Yogyakarta and Makassar, Indonesia. *Frontiers in Political Science*, 7, Article 1553177. <https://doi.org/10.3389/fpos.2025.1553177>
- Hossain, M. I., & Hasan, R. (2024). Smart cities: Cybersecurity concerns. In J. R. Vacca (Ed.), *Computer and information security handbook* (4th ed., pp. 1397–1412). Morgan Kaufmann. <https://doi.org/10.1016/B978-0-443-13223-0.00089-8>
- Humayun, M., Jhanjhi, N. Z., Alamri, M. Z., & Khan, A. (2020). Smart cities and digital governance. In V. Ponnusamy, K. Rafique, & N. Z. Jhanjhi (Eds.), *Employing Recent Technologies for Improved Digital Governance* (pp. 87–106). IGI Global. <https://doi.org/10.4018/978-1-7998-1851-9.ch005>
- Ilyas, M. (2021). IoT applications in smart cities. In *2021 IEEE International Conference on Electronic Communications, Internet of Things and Big Data (ICEIB)* (pp. 44–47). IEEE. <https://doi.org/10.1109/ICEIB53692.2021.9686400>
- Iqbal, M., & Matulevičius, R. (2019). Comparison of blockchain-based solutions to mitigate data tampering security risk. In C. Di Ciccio, R. Gabryelczyk, L. García-Bañuelos, T. Hernaus, R. Hull, M. Indihar Štemberger, A. Kő, & M. Staples (Eds.), *Business process management: Blockchain and Central and Eastern Europe Forum (Lecture notes in business information processing, Vol. 361)* (pp. 13–28). Springer. https://doi.org/10.1007/978-3-030-30429-4_2
- Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2022). Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. *Information Systems Frontiers*, 24(2), 393–414. <https://doi.org/10.1007/s10796-020-10044-1>
- Jaakonmäki, R., vom Brocke, J., Dietze, S., Drachsler, H., Fortenbacher, A., Helbig, R., Kickmeier-Rust, M., Marenzi, I., Suarez, A., & Yun, H. (2020). Responsible Cooking with Learning Analytics. In R. Jaakonmäki, J. vom Brocke, S. Dietze, H. Drachsler, A. Fortenbacher, R. Helbig, M. Kickmeier-Rust, I. Marenzi, A. Suarez, & H. Yun (Eds.), *Learning Analytics Cookbook How to Support Learning Processes Through Data Analytics and Visualization* (pp. 15–30). Springer. https://doi.org/10.1007/978-3-030-43377-2_3
- Jarour, A., & Mocanu, M. (2025). Smart urban governance frameworks: A comparative analysis. *UPB*

- Scientific Bulletin, Series C: Electrical Engineering and Computer Science*, 87(3), 95–106. https://www.scientificbulletin.upb.ro/static/pdfs/fulleab_252809.pdf
- Jayanthi, M., & Pravallika Reddy, C. (2020). Theoretical design and experimental study for urban data management using energy-saved IoT big data. In R. Chillarige, S. Distefano, & S. Rawat (Eds.), *Advances in computational intelligence and informatics: ICACII 2019 (Lecture notes in networks and systems, Vol. 119)* (pp. 285–292). Springer. https://doi.org/10.1007/978-981-15-3338-9_33
- Jebbar, H., El Mohadab, M., & Boutkhoul, O. (2024). Smart cities: Literature review and bibliometric analysis. *International Journal on Technical and Physical Problems of Engineering*, 16(59), 321–330. <https://www.ijtp.com/IJTPE/Issues/2020/IJTPE-2024/IJTPE-Issue59-Vol16-No2-Jun2024/41-IJTPE-Issue59-Vol16-No2-Jun2024-pp321-330.pdf>
- Jyothi, V., Sreelatha, T., Thiyagu, T. M., Sowndharya, R., & Arvinth, N. (2024). A data management system for smart cities leveraging artificial intelligence modeling techniques to enhance privacy and security. *Journal of Internet Services and Information Security*, 14(1), 37–51. <https://doi.org/10.58346/JISIS.2024.11.003>
- Kasar, S., & Kshirsagar, M. (2021). Open challenges in smart cities: Privacy and security. In S. C. Tamane, N. Dey, & A.-E. Hassanien (Eds.), *Security and privacy applications for smart city development (Studies in systems, decision and control, Vol. 308)* (pp. 25–36). Springer. https://doi.org/10.1007/978-3-030-53149-2_2
- Kitchin, R., & Dodge, M. (2019). The (in)security of smart cities: Vulnerabilities, risks, mitigation, and prevention. *Journal of Urban Technology*, 26(2), 47–65. <https://doi.org/10.1080/10630732.2017.1408002>
- Kontogeorgis, G., & Varotsis, N. (2021). Reinstating Greek e-governance: A framework for e-government benchmarking, improvement and government policies. *Public Administration Issues*, 6, 103–127. <https://doi.org/10.17323/1999-5431-2021-0-6-103-127>
- Kourtiti, K., Nijkamp, P., & Steenbruggen, J. (2017). The significance of digital data systems for smart city policy. *Socio-Economic Planning Sciences*, 58, 13–21. <https://doi.org/10.1016/j.seps.2016.10.001>
- Krishnan, S., & Ganesan, L. P. (2021). Smart cities with blockchain technology: A comprehensive survey. In S. Krishnan, V. E. Balas, E. G. Julie, Y. H. Robinson, & R. B. T.-B. for S. C. Kumar (Eds.), *Blockchain for Smart Cities* (pp. 1–15). Elsevier. <https://doi.org/10.1016/B978-0-12-824446-3.00016-8>
- Kushwaha, S. (2023). Challenges and opportunities in the development of a smart grid system in India. In R. Viral, D. Asija, & S. Salkuti (Eds.), *Big Data Analytics Framework for Smart Grids* (pp. 26–40). CRC Press. <https://doi.org/10.1201/9781032665399-2>
- Lawelai, H., Purnomo, E. P., Nurmandi, A., Jovita, H., & Baulete, E. M. (2025). Cybersecurity policy on smart city infrastructure: A mapping of new threats and protections. *Journal of Science and Technology Policy Management*. Advance online publication. <https://doi.org/10.1108/JSTPM-09-2024-0359>
- Linkov, I., Anklam, E., Collier, Z. A., DiMase, D., & Renn, O. (2014). Risk-based standards: Integrating top-down and bottom-up approaches. *Environment Systems and Decisions*, 34(1), 134–137. <https://doi.org/10.1007/s10669-014-9488-3>
- Liu, Z., & Wu, J. (2023). A review of the theory and practice of smart city construction in China. *Sustainability*, 15(9), Article 7161. <https://doi.org/10.3390/su15097161>
- Meijer, A., & Bolívar, M. P. R. (2016). Governing the smart city: A review of the literature on smart urban governance. *International Review of Administrative Sciences*, 82(2), 392–408. <https://doi.org/10.1177/0020852314564308>
- Melaku, H. M. (2023). A dynamic and adaptive cybersecurity governance framework. *Journal of Cybersecurity and Privacy*, 3(3), 327–350. <https://doi.org/10.3390/jcp3030017>
- Ngossaha, J. M., Ngouna, R. H., Archimède, B., & Ndjodo, M. F. (2018). A Simulation Model for Risk Assessment in a Smart Mobility Ecosystem based on the Inoperability Input-Output Theory. In J. J. Padilla & C. J. Lynch (Eds.), *Proceedings of the 50th Computer Simulation Conference* (Vol. 50, Issue 10, pp. 362–371). Society for Modeling and Simulation International (SCS). <https://doi.org/10.22360/SummerSim.2018.SCSC.053>
- Petersen, K., Feldt, R., Mujtaba, S., & Mattsson, M. (2008). Systematic mapping studies in software engineering. In G. Visaggio, M. T. Baldassarre, S. Linkman, & M. Turner (Eds.), *Proceedings of the 12th International Conference on Evaluation and Assessment in Software Engineering (EASE 2008)*

- (pp. 1–10). BCS Learning & Development. <https://doi.org/10.14236/ewic/EASE2008.8>
- Prakoso, V., Lawelai, H., Nurmandi, A., Purnomo, E. P., & Jovita, H. (2023). Research trends, topics, and insights on network security and the Internet of Things in smart cities. *Jurnal Studi Ilmu Pemerintahan*, 4(2), 191–206. <https://jurnal-umbuton.ac.id/index.php/jsip/article/view/4707>
- Raghav, A., Singh, B., Raghav, R., & Edina, K. D. (2025). AI and robotics in smart city governance: Ethical and legal pathways for sustainable urbanization. In K. Ravesangar, C. Kaunert, B. Singh, S. Lal, & M. Arora (Eds.), *Machine Learning and Robotics in Urban Planning and Management* (pp. 1–24). IGI Global. <https://doi.org/10.4018/979-8-3693-9410-6.ch001>
- Rajalakshmi, N. R., Thanga Mariappan, L., Saravanan, K., & Mahesh Nayak, B. (2023). Blockchain-based big data platforms for sustainable smart cities. In S. Krishnan, R. Kumar, & V. E. Balas (Eds.), *Green blockchain technology for sustainable smart cities* (pp. 263–276). Elsevier. <https://doi.org/10.1016/B978-0-323-95407-5.00001-3>
- Ravikumar, R., Singhal, S., Betgeri, S., & Singh, S. K. (2024). Strategies for mitigating security concerns in IoT-enabled smart cities. In S. Singh, S. Tanwar, R. Jadeja, S. Singh, & Z. Polkowski (Eds.), *Secure and Intelligent IoT-Enabled Smart Cities* (pp. 239–273). IGI Global. <https://doi.org/10.4018/979-8-3693-2373-1.ch012>
- Salnitri, M., Angelopoulos, K., Pavlidis, M., Diamantopoulou, V., Mouratidis, H., & Giorgini, P. (2020). Modelling the interplay of security, privacy and trust in sociotechnical systems: A computer-aided design approach. *Software and Systems Modeling*, 19(2), 467–491. <https://doi.org/10.1007/s10270-019-00744-x>
- Schotten, M., El Aisati, M., Meester, W. J. N., Steiginga, S., & Ross, C. A. (2017). A brief history of Scopus: The world's largest abstract and citation database of scientific literature. In F. J. Cantú-Ortiz (Ed.), *Research analytics: Boosting university productivity and competitiveness through scientometrics* (pp. 31–58). Auerbach Publications. <https://doi.org/10.1201/9781315155890>
- Sidorenko, E., Bartsits, I., & Khisamova, Z. (2019). Effektivnost' tsifrovogo gosudarstvennogo upravleniya: Teoreticheskie i prikladnye aspekty [The efficiency of digital public administration assessing: Theoretical and applied aspects]. *Public Administration Issues*, 2019(2), 93–114. <https://doi.org/10.17323/1999-5431-2019-0-2-93-114>
- Subrahmanyam, S. (2025). Data governance and privacy in smart cities. In A. Sharma, V. Mansotra, & P. Singh (Eds.), *Citizen-centric artificial intelligence for smart cities* (pp. 433–456). IGI Global. <https://doi.org/10.4018/979-8-3693-7832-8.ch017>
- Suresh Kumar, K., Prabakaran, D., Senthil Kumaran, R., & Yamuna, I. (2022). Privacy and security of smart systems. In S. L. Tripathi, S. Ganguli, T. Magradze, & A. Kumar (Eds.), *Intelligent green technologies for sustainable smart cities* (pp. 291–315). Wiley. <https://doi.org/10.1002/9781119816096.ch14>
- Verma, R., Dhanda, N., & Nagar, V. (2022). Enhancing and optimizing security of IoT systems using different components of Industry 4.0. *International Journal of Engineering Trends and Technology*, 70(7), 147–157. <https://doi.org/10.14445/22315381/IJETT-V70I7P216>
- Vitunskaitė, M., He, Y., Brandstetter, T., & Janicke, H. (2019). Smart cities and cyber security: Are we there yet? A comparative study on the role of standards, third party risk management and security ownership. *Computers & Security*, 83, 313–331. <https://doi.org/10.1016/j.cose.2019.02.009>
- Wang, X., Chen, Y., Liu, Y., Yao, L., Estill, J., Bian, Z., Wu, T., Shang, H., Lee, M. S., Wei, D., Tian, J., Ma, B., Wang, Y., Tian, G., & Yang, K. (2019). Reporting items for systematic reviews and meta-analyses of acupuncture: The PRISMA for acupuncture checklist. *BMC Complementary and Alternative Medicine*, 19(1), Article 208. <https://doi.org/10.1186/s12906-019-2624-3>
- Wirtz, B. W., & Weyerer, J. C. (2017). Cyberterrorism and cyber attacks in the public sector: How public administration copes with digital threats. *International Journal of Public Administration*, 40(13), 1085–1100. <https://doi.org/10.1080/01900692.2016.1242614>
- Wu, Y. C., Sun, R., & Wu, Y. J. (2020). Smart city development in Taiwan: From the perspective of the information security policy. *Sustainability*, 12(7), Article 2916. <https://doi.org/10.3390/su12072916>
- Xagoraris, L., Kogias, D., & Karkazis, P. (2024). A review of zero trust security framework (ZTF) for sustainable and resilient smart cities. In *Proceedings of the 27th Pan-Hellenic Conference on Progress in Computing and Informatics* (pp. 269–273). Association for Computing Machinery. <https://doi.org/10.1145/3635059.3635102>

- Xihua, Z., & Goyal, S. B. (2022). Security and privacy challenges using IoT-blockchain technology in a smart city: Critical analysis. *International Journal of Electrical and Electronics Research*, 10(2), 190–195. <https://doi.org/10.37391/IJEER.100224>
- Yemanov, V., Dzyana, H., Dzyanyi, N., Dolinchenko, O., & Didych, O. (2023). Modelling a public administration system for ensuring cybersecurity. *International Journal of Safety and Security Engineering*, 13(1), 81–88. <https://doi.org/10.18280/ijssse.130109>
- Yigitcanlar, T. (2015). Smart cities: An effective urban development and management model? *Australian Planner*, 52(1), 27–34. <https://doi.org/10.1080/07293682.2015.1019752>
- Zhu, J., & Liu, W. (2020). A tale of two databases: The use of Web of Science and Scopus in academic papers. *Scientometrics*, 123(1), 321–335. <https://doi.org/10.1007/s11192-020-03387-8>