DIGITAL THREATS IN SMART CITIES – A COMPREHENSIVE REVIEW IN THE CONTEXT OF ARTIFICIAL INTELLIGENCE

Michał Madera[1]
Rzeszow University of Technology, Poland

Andrzej Paszkiewicz[2]
Rzeszow University of Technology, Poland

Lesław Bańdur[3]
Rzeszow City Hall, IT and Telecommunications Service Office

Sławomir Świder[4]
Rzeszow City Hall, IT and Telecommunications Service Office

DOI: https://doi.org//10.62140/MMAPLBSS1062025

Abstract: Smart cities are a new approach to the innovation of the urban environment, which is impossible to imagine without the latest technologies, including Artificial Intelligence (AI) and the Internet of Things (IoT). These interconnected systems offer creative solutions to various challenges in significant sectors like energy, transportation, safety, and healthcare. Thus, smart cities can be defined as dynamic ecosystems based on data-driven technologies

[1] Assistant Professor at Rzeszów Univerity of Technology. E-mail: michalmadera@gmail.com Link ORCID: https://orcid.org/0000-0002-4474-682X

[2] Assistant Professor at Rzeszów Univerity of Technology. E-mail: andrzejp@prz.edu.pl

Link ORCID: https://orcid.org/0000-0001-7573-3856

[3] Director of IT and Telecommunications Service Office at Rzeszow City Hall. E-mail: leslaw.bandur@erzeszow.pl

[4] Deputy Director of IT and Telecommunications Service Office at Rzeszow City Hall. E-mail: swiders@erzeszow.pl

for real-time decision-making, resource management, and citizen engagement. However, the increase in the integration of AI and IoT comes with many challenges. This paper seeks to present both sides of these innovations, which can improve the urban ecosystem while also increasing its sustainability and vulnerability. Key risks include data breaches, algorithmic bias, and cyber threats to critical infrastructure that can jeopardize trust and resilience. The study also notes the lack of harmony in the evolution of research on AI-related developments and cybersecurity, which underpins the need for equilibrium in innovation. This paper aims to contribute to the understanding of the integration of AI in smart cities and their core systems, such as energy networks, transportation, and healthcare, through an assessment of current research and practices. It also stresses the significance of strong governance, ethical principles, and risk management. Thus, the potential of smart cities as safe, inclusive, and adaptive environments for future generations can be fulfilled. In this way, the paper aims to offer a way forward for the development of secure, fair, and creative urban environments in the networked society.
Keywords: smart city, digital threats, artificial intelligence, urban efficiency, cybersecurity

INTRODUCTION

Smart cities, a hallmark of the modern digital age, hold the potential to significantly improve the quality of life in urban areas. By integrating digital technologies and the Internet of Things (IoT), these cities create interconnected systems that enhance urban efficiency, sustainability, and ultimately, the well-being of their citizens (Naphade et al. 2011). This transformative approach optimizes traditional infrastructure and redefines the relationship between citizens and their urban environment, offering a hopeful vision for the future. A defining feature of smart cities is their reliance on IoT, a network of interconnected sensors, devices, and systems that generate and exchange real-time data. This data forms the foundation for informed decision-making, enabling adaptive responses to urban challenges. Whether through intelligent traffic management systems that alleviate congestion, smart grids that optimize energy consumption, or environmental monitoring systems that track air and water quality, IoT provides the critical infrastructure for achieving urban resilience and sustainability.

One of the formal definitions of the smart city, dated 2010, is the following: a city "connecting the physical infrastructure, the information-technology infrastructure, the social infrastructure, and the business infrastructure to leverage the collective intelligence of the city" (Harrison et al. 2010). Later, in 2014, we found another comprehensive definition

emphasizing sustainability and ICT: “a smart sustainable city is an innovative city that uses information and communication technologies (ICTs) and other means to improve quality of life, the efficiency of urban operations and services, and competitiveness while ensuring that it meets the needs of present and future generations with respect to economic, social and environmental aspects” (Kondepudi et al. 2014). While AI's historical evolution has showcased significant milestones, recent advancements in neural networks, cognitive computing, and machine learning have unlocked unprecedented capabilities in energy management, monitoring, and optimization. Starting in the 2020s, the combination of artificial intelligence with 5G networks and sensor systems creates a promising foundation for next-generation smart city services (Şerban, Lytras 2020). Moreover, digital technologies such as AI, machine learning, and big data analytics amplify the capabilities of smart cities by processing vast volumes of urban data. These technologies enable predictive insights, automated operations, and personalized services, empowering city authorities to anticipate and address issues proactively. The integration of IoT and digital technologies in smart cities creates a dynamic ecosystem characterized by interoperability, scalability, and citizen-centricity. However, these advancements also introduce significant challenges. Data privacy, cybersecurity, and socio-economic inclusivity concerns underscore the need for robust governance frameworks and ethical considerations. Without addressing these challenges, smart cities' promise may exacerbate existing inequalities and vulnerabilities.

In that domain, one could expect a significant demand for scientific research to guide innovation toward the most impactful directions. The analysis of publication trends for the keyword "smart city" in ScienceDirect (*ScienceDirect.com | Science, health and medical journals, full text articles and books.*) and IEEE Xplore (*IEEE Xplore*) repositories reveal a consistent pattern in research output for the last 15 years. In ScienceDirect, the growth rate is generally exponential, particularly notable between 2015 and 2024, where the increase from 3,520 to 16,118 reflects a surge in interest and research output related to smart cities. The IEEE growth rate is more volatile. After a peak in 2015, the number of publications declined slightly until 2020 before increasing again. This suggests that while interest remains, it may not be growing at the same pace as seen in ScienceDirect. While both databases are essential in academic research, ScienceDirect offers a broader multidisciplinary range of publications, whereas IEEE Xplore focuses on technical literature, primarily in engineering and computer science.

This increase in publication trends highlights the importance of examining the technological advancements driving smart cities and the broader implications of their

adoption, including social, economic, and environmental impacts. The 2018 report "Smart Cities: Digital Solutions for a More Livable Future" by the McKinsey Global Institute assessed how smart cities equipped with advanced technologies address urban challenges (Woetzel et al. 2018). The findings revealed that smart cities' positive impact on quality of life exceeded prior expectations. Key improvements were noted in social inclusion, civic participation, employment opportunities, and the cost of living. According to the report, smart cities demonstrated significant progress in health and public safety, reducing mortality rates by 8–10% and improving emergency response times by 20–35%. These advancements also resulted in an 8–15% decrease in healthcare costs and a 10–15% reduction in greenhouse gas emissions. These developments have collectively enhanced urban efficiency and sustainability, creating more innovative, livable cities.

In addition to the many benefits of digitalization in smart cities, significant digital threats also arise that must be addressed. The growing dependence on AI systems in future cities presents both opportunities and risks. Smart cities integrate AI into critical infrastructure, despite this dependence also creating vulnerabilities at completely new levels. AI-driven systems are susceptible to cyberattacks, data breaches, and system failures, which could disrupt essential services and compromise public trust.

The comparison of Google Search Trends for "artificial intelligence" (AI) and "cybersecurity" over the past five years reveals a growing divergence, with AI gaining significantly more attention for the last 5 years (*Google Trends for "artificial intelligence" and "cybersecurity"* 2025). This reflects the rapid advancements in AI technologies and their transformative potential, particularly in domains such as smart cities. However, the steadier, less pronounced growth in interest in cybersecurity highlights a critical gap: while AI systems are being deployed at an unprecedented rate, their security implications often receive insufficient attention. Interestingly, drilling down into regions reveals that interest in "cybersecurity" surpasses "artificial intelligence" in regions such as North America, which is opposite to Europe. Although exploring the reasons for this regional variation lies beyond the scope of this research, it is notable that enthusiasm for AI versus concerns about its risks, such as cybersecurity, may vary significantly across different cultural and socio-political contexts.

Artificial intelligence begins to play a pivotal role in optimizing urban systems, managing resources, and enhancing the quality of life in smart cities. However, these interconnected systems are highly vulnerable to a range of cyber threats, including data breaches, ransomware attacks, and exploitation of IoT devices (Wolniak, Stecuła 2024;

Haugaard 2020). Despite the transformative potential of AI, the disparity in focus between AI-driven innovations and cybersecurity measures highlights an imbalance that could undermine the safe and sustainable implementation of smart city solutions. Addressing these vulnerabilities requires the integration of robust cybersecurity measures into the design and deployment of AI technologies from the outset. A holistic approach that prioritizes resilience, privacy, and trust is essential to safeguard urban systems. Additionally, the widespread adoption of AI raises concerns about algorithmic bias, privacy violations, and unintended consequences in automated decision-making. These risks are particularly acute in urban environments, where the interconnected nature of systems amplifies the potential for cascading errors or malicious intrusions.

This study investigates the risks associated with AI use in smart cities, emphasizing the need to address both technical vulnerabilities and broader ethical and regulatory challenges. Following the Introduction, Section 2 examines the role of AI in enhancing smart city systems, providing a framework for analyzing smart cities through core system divisions. Section 3 addresses the challenges arising from the interconnection of these subsystems. Section 4 explores digital threats within the previously defined core systems, while Section 5 highlights threats that have already materialized. Ethical challenges are discussed in Section 6, with the study's summary and conclusions presented in Section 7.

The Role of AI

The integration of Artificial Intelligence (AI) in smart cities has led to transformative improvements in urban efficiency, sustainability, and citizen well-being. Multiple core smart city systems increasingly act as both generators and consumers of information, often interacting directly or indirectly. As a result, a smarter city can be conceptualized as a "system of systems" of enormous complexity, benefiting from AI across diverse domains.

We propose dividing core systems into “Urban Infrastructure & Resource Systems” and “Public Services & Citizen Well-being”, which reflects a logical grouping based on functionality and objectives. The former focuses on managing physical and technological infrastructure, such as energy, transportation, and housing, ensuring resource optimization and sustainability. Meanwhile, the latter addresses citizen-centric services, including public health, safety, education, and social engagement, aiming to improve quality of life and inclusivity. This division highlights the dual priorities of smart cities: efficient resource management and enhanced citizen well-being. For example, Transport and Urban Mobility underpins both economic activities and accessibility, while Public Safety and Crisis

Management ensures resilience against disruptions. Similarly, Digital Systems and Data Management underpin all other systems, enabling interoperability and real-time decision-making. By structuring smart city systems in this manner, the framework emphasizes the holistic and integrated nature of AI-driven urban ecosystems. This approach facilitates targeted innovation, ensuring that technological advancements effectively address infrastructure efficiency and citizen needs.

Urban Infrastructure and Resource Systems

AI-driven solutions are crucial in optimizing resource utilization and infrastructure management, enabling smarter cities with reduced environmental footprints. In energy and water management, AI enhances systems through smart grids, predictive analytics, and optimized recycling, improving efficiency and sustainability. AI also transforms transport and mobility by enabling real-time traffic prediction, dynamic routing, and shared mobility platforms, reducing congestion and emissions. For urban infrastructure, AI facilitates continuous monitoring of assets such as roads and bridges, prioritizing maintenance to extend lifespans. Smart parking systems and building automation further enhance urban accessibility and energy efficiency. These applications collectively support sustainable urban growth and an improved quality of life for city residents (Wolniak, Stecuła 2024).

Public Services and Citizen Well-being

AI enhances the quality of life in smart cities by transforming public services into adaptive systems. In public safety, AI-powered surveillance detects threats in real time, while predictive analytics help anticipates disasters and improve crisis response. In healthcare, AI-driven telemedicine provides remote monitoring and diagnostics, increasing accessibility and optimizing resource allocation during challenges like pandemics. AI also advances education and citizen engagement through personalized learning platforms and tools for participatory governance, such as digital budgeting and community feedback systems. By modernizing these services, AI helps create smarter, more responsive cities that prioritize citizen well-being (Wolniak, Stecuła 2024).

Economy and Innovation

AI fosters economic growth and innovation in smart cities by empowering local economies and enhancing urban services. AI-enabled platforms provide tools for entrepreneurs and small businesses to optimize operations, access market insights, and

connect with broader audiences. These platforms improve resource allocation, supply chain efficiency, and pricing strategies, boosting competitiveness.

Intelligent systems drive advancements in urban services by supporting digital government portals and automated administrative processes, streamlining service delivery and reducing costs. Predictive analytics further aid urban economic planning by providing insights into trends and labor markets, enabling smarter policies for sustainable growth and employment.

Digital Systems and Data Management

Efficient and secure data management is vital for smart city operations, with AI ensuring data integrity, accessibility, and interoperability. AI-powered algorithms enhance cybersecurity by detecting vulnerabilities and protecting sensitive data, which is critical given the vast real-time data generated by interconnected IoT devices. AI also enables urban digital twins, virtual models of city systems that simulate urban functions in real-time. These tools help planners analyze policy impacts, optimize resources, and predict system failures. By securing and streamlining data sharing, AI supports cohesive urban ecosystems, enhances decision-making, and fosters resilient, adaptive environments.

Challenges of Interconnection of Subsystems

The interconnection of subsystems in a smart city, such as transportation, energy, water management, public safety, and healthcare, creates a complex ecosystem of interdependent technologies. While this integration enhances efficiency and coordination, it also presents significant challenges. Table 1 summarizes the example challenges, followed by implementation examples.

Challenge	Solution
Smart city subsystems from different vendors often lack seamless integration due to varying technologies and protocols, hindering data exchange.	AI-powered middleware bridges these gaps by translating data and unifying communication. It enables real-time coordination between smart traffic lights and EV charging stations, optimizing energy use during peak hours.
The immense data generated by interconnected subsystems like sensors, surveillance, and IoT devices poses	AI efficiently processes and analyzes large data volumes in real time. For instance, AI-powered predictive analytics can identify

significant challenges in storage, processing, and real-time analysis, critical for smooth operations.	traffic flow patterns, optimizing public transport schedules and road infrastructure to reduce congestion
Interconnected systems expand the attack surface for cyber threats, as vulnerabilities in one subsystem can cascade to others. For example, a cyberattack on a water management system could disrupt interconnected energy distribution networks.	AI mitigates cybersecurity risks by detecting anomalies and using predictive threat modeling. For instance, AI algorithms monitor network activity to identify unusual patterns, enabling rapid response to cyberattacks and minimizing damage.
The failure of one subsystem can have cascading effects on others. For example, a blackout in the energy grid can disrupt public transportation, emergency services, and communication networks.	Resilience models simulate failure scenarios and recommend measures to prevent cascading effects. Digital twins can model energy outages' impacts on transportation, helping planners implement alternative routes.
Interconnected systems collect sensitive citizen data, risking privacy violations, such as misuse of health information when integrating healthcare and public safety data.	AI ensures privacy through automated anonymization and encryption, safeguarding personal data while enabling secure subsystem integration.
Smart city subsystems often involve multiple stakeholders, including government agencies, private companies, and citizens, making coordination and decision-making complex.	AI-powered dashboards can support decisions by delivering real-time information on energy, transportation, and safety, enabling collaborative, informed decisions.

Table 1. Example Smart City Threats' Challenges and AI-powered Solution examples.

Implementation examples:

- **Barcelona** uses AI to integrate data from its IoT-enabled urban infrastructure, including smart water systems and waste management, to optimize resource allocation and improve service delivery. (Haugaard 2020)
- **Singapore's** The Smart Nation initiative showcases AI-powered digital twins, like the Virtual Singapore project, which simulates interconnected systems such as transport and

urban planning. This high-resolution virtual model integrates real-time data to simulate scenarios, optimize solutions, and support data-driven decisions for resilience and smart city growth. (Lopes 2024)

- **New York City** Cyber Command (NYC3) has implemented a robust, scalable cloud infrastructure utilizing Google Cloud to enhance the security of the city's digital services. Facing approximately 90 billion cyber events weekly, NYC3 employs artificial intelligence and automated decision-making tools to distill these events into a manageable number of actionable items. (*NYC Cyber Command - Google AI for Public Sector*)

Digital Threats in Core Smart City Systems

The integration of advanced technologies in smart cities introduces significant cybersecurity challenges across core systems, potentially undermining the efficiency, safety, and trust of urban infrastructure. These challenges are closely tied to the interconnected nature of smart city subsystems, which rely on real-time data exchange and IoT devices. Below, we outline the most critical cybersecurity threats as they pertain to the core systems of smart cities:

1. Smart Energy and Natural Resource Management. Smart grids and water management systems are increasingly vulnerable to cyberattacks targeting their interconnected networks. A successful attack on a smart grid could disrupt energy distribution, leading to widespread power outages and cascading failures in other systems (Achaal et al. 2024). Similarly, water management systems are susceptible to unauthorized access or ransomware attacks, which could compromise water quality or availability (Hassanzadeh et al. 2020). These threats highlight the need for robust encryption, real-time anomaly detection, and secured IoT devices to protect critical resource systems.

2. Transport and Urban Mobility. Intelligent traffic management systems and shared mobility platforms rely heavily on IoT devices and real-time data to optimize routes and reduce congestion. Cyber threats in this domain include GPS spoofing, which could misguide autonomous vehicles, and attacks on traffic signal networks, causing widespread disruptions (Mecheva, Kakanakov 2020). Additionally, breaches in shared mobility platforms may expose user data or disable services. Addressing these risks requires implementing secure communication protocols and AI-driven predictive maintenance to identify vulnerabilities before exploitation.

3. Waste Management and Sustainability. Cyber threats to waste management systems often target IoT-enabled devices, such as sensors monitoring bin fill levels or

vehicles used in waste collection. Unauthorized access to these systems can disrupt operations, leading to inefficient waste collection and increased costs. Moreover, compromised systems could be exploited for malicious purposes, such as data breaches revealing operational details. Strengthening cybersecurity measures, including device authentication and secure firmware updates, is critical for maintaining reliable waste management (Brighente et al. 2024).

4. Public Safety and Crisis Management. Public safety systems, including surveillance networks and emergency response platforms, are prime targets for cyberattacks due to the sensitivity of the data they handle. Hackers could exploit vulnerabilities in AI-driven surveillance systems to disable monitoring capabilities or manipulate video feeds. Similarly, breaches in emergency response platforms could delay critical interventions, exacerbating the impact of crises. Employing AI-powered threat detection and end-to-end data encryption can mitigate these risks (*NIST Identifies Types of Cyberattacks That Manipulate Behavior of AI Systems* 2024; *Groundbreaking Framework for the Safe and Secure Deployment of AI in Critical Infrastructure Unveiled by Department of Homeland Security | Homeland Security* 2024).

5. Smart Buildings and Housing Infrastructure. Automation systems in smart buildings, such as those controlling lighting, heating, and ventilation, are increasingly exposed to cyber threats. Attacks on these systems could result in unauthorized access to private residences or the disruption of essential services. Furthermore, vulnerabilities in building monitoring systems could compromise data integrity, leading to incorrect maintenance decisions. Robust network segmentation and AI-driven intrusion detection systems are essential for safeguarding smart buildings (Li et al. 2023; *Artificial Intelligence in Building Management*).

6. Education, Culture, and Citizen Engagement. Digital platforms supporting education and citizen engagement often collect personal data, making them attractive targets for data breaches and identity theft (Kim et al. 2023). Cyberattacks on these platforms could compromise citizen trust and participation, undermining the inclusivity of smart city initiatives. Implementing strict data privacy regulations and AI-driven monitoring tools can help secure these platforms against unauthorized access.

7. Urban Infrastructure Optimization. Systems managing urban infrastructure, such as smart street lighting and public space management, are vulnerable to denial-of-service (DoS) attacks and unauthorized control. For instance, disabling smart lighting could create safety hazards, while compromised public space management systems could disrupt urban

planning. Strengthening cybersecurity through redundant systems and AI-driven threat mitigation can enhance resilience against these threats. (Hofer, Russo 2021)

8. Economy and Innovation. Smart commerce platforms and urban innovation hubs are susceptible to cyberattacks targeting payment systems, intellectual property, and sensitive commercial data. Such breaches could disrupt local economies and discourage innovation. Implementing AI-powered fraud detection and secure blockchain-based transactions can protect economic activities in smart cities.(Pranto et al. 2022)

9. Public Health and Social Care. Telemedicine platforms and health monitoring systems handle sensitive personal data, making them prime targets for ransomware and data breaches. Cyberattacks in this domain could jeopardize patient safety by disrupting critical health services. Comprehensive cybersecurity measures, such as data encryption and AI-driven anomaly detection, are vital to protect these systems.(Seh et al. 2020)

10. Digital Systems and Data Management. As the backbone of all smart city systems, digital platforms and IoT devices are particularly vulnerable to cyber threats (Kim et al. 2023). Unauthorized access to data management systems or digital twins could lead to widespread disruptions and compromise the integrity of interconnected systems. Employing advanced AI algorithms for real-time threat detection, secure data sharing, and IoT device management is crucial for ensuring the stability and security of smart city operations.

By addressing these cybersecurity challenges across core systems, smart cities can safeguard their infrastructure and services, ensuring resilience, efficiency, and trust in urban environments.

Materialized digital threats

The cybersecurity landscape has seen a significant increase in incidents over recent years, affecting organizations across various sectors. In 2024, the average cost of a data breach reached $4.88 million, marking the highest average on record. Notably, 88% of these breaches were attributed to human error (*Cybersecurity Statistics and Trends [updated 2024]*). Small and medium-sized businesses (SMBs) are particularly vulnerable, with 48% experiencing cyberattacks. However, 43% of these businesses struggle to understand the necessary security measures to protect themselves (*Cybersecurity statistics to lose sleep over in 2025*). Globally, cyberattacks increased by 30% in the second quarter of 2024, averaging 1,636 weekly attacks per organization (*Key Cyber Security Statistics for 2025*). In the United States, the federal government allocated $12.72 billion to cybersecurity spending for fiscal year 2024, excluding the Department of Defense (*Cybersecurity statistics to lose sleep over in 2025*). These

statistics underscore the escalating frequency and financial impact of cyber threats, highlighting the critical need for robust cybersecurity measures across all sectors.

The integration of advanced technologies in smart cities has led to significant cybersecurity challenges across various sectors. Below are real-world incidents illustrating vulnerabilities in three key areas:

- In the United Kingdom, concerns have been raised about the security of smart meters. Experts warn that these devices could be exploited to spy on households, as the government plans to allow energy data sharing with other companies to help lower prices. This has led to warnings for consumers to be cautious about the potential intrusion of smart meters. (Eastwood 2025)
- In Europe, the transportation sector was the target of about 11% of all cyber-attacks over the year to the end of June 2024, according to a survey published in September by the European Agency for Cyber Security (ENISA). This level of targeting was topped only by attacks on the public sector (19%) and was ahead of the financial sector (9%). (Gerrish 2024)
- A study published in 2023 investigated the security and privacy issues of Smart Waste Management Systems (SWMSs) from a cyber-physical system perspective (Brighente et al. 2024). The research highlighted that SWMSs may be subject to different cyber-physical threats due to the interconnection of information and operational technologies, emphasizing the need for robust cybersecurity measures in this sector.
- In March 2018, Atlanta, Georgia, experienced a significant ransomware attack that severely disrupted municipal operations. The attackers deployed the SamSam ransomware, encrypting numerous city systems and demanding a ransom of approximately $51,000 in Bitcoin. Critical services, including utility billing, court records, and internal communications, were affected, forcing city employees to revert to manual processes. The attack resulted in extensive data loss and recovery costs estimated at $2.7 million. This incident underscores the vulnerabilities inherent in urban digital infrastructures and the substantial impact cyberattacks can have on essential public services. (*Atlanta city computer network remains hobbled by cyberattack* 2018)

Ethical challenges

The employment of AI in smart cities poses important ethical and privacy issues that become even more important when these systems are based on the analysis of consumers' data. It is therefore important to set guidelines and rules for the use of data, privacy, and the

ethical use of AI in implementing these technologies to increase the chances of using these technologies for increased security in cities. The protection of the privacy and autonomy of the citizens is a concern that cannot be overlooked as smart cities try to improve security through the use of AI.The application of AI in smart cities comes with challenges, and one of the primary challenges is the need for a skilled workforce to design, deploy, and manage AI-based safety measures. Smart cities, therefore, have to promote training and capacity building for this shortage in order to work with academic institutions, research institutions, and industry partners to share and develop knowledge in this area (Vasileiou 2020). These efforts will guarantee the ethical use of AI technologies in urban systems. However, the use of AI in smart cities is not without its challenges, some of which include data quality, model explainability, and public trust. In order to build the public's confidence in the use of AI, the AI models and decision-making processes must be understandable (Laufs et al. 2020). Moreover, the proper deployment of AI demands periodic assessment to guarantee that the technology complies with privacy policies and to address new risks in a fast changing technological environment. Thus, the integration of ethical principles into the design of smart cities can help in improving security, robustness and trust through the use of AI while at the same time promoting accountability and equity. The development of smart cities can be described as a collaborative and inclusive process that enables urban areas to develop and improve solutions that would make our communities safer and fairer in the digital environment.

CONCLUSIONS

This paper comprehensively reviews the role of AI and the IoT in smart cities. It highlights their transformative potential in enhancing urban efficiency, sustainability, and citizen well-being. Real-time decision-making, resource optimization, and citizen-centric services are possible by the integration of advanced technologies into urban systems. While this paper emphasizes the dual nature of these innovations, it acknowledges risks related to their adoption. However, this paper emphasizes the dual nature of these innovations, acknowledging the significant risks introduced by their adoption. Thus, challenges such as data breaches, cyberattacks, algorithmic bias, and the socio-economic implications of rapid technological advancements are explored. Through a detailed analysis of publication trends, real-world case studies, and technological frameworks, the study underscores the need for robust cybersecurity measures, governance frameworks, and ethical considerations to ensure secure and sustainable implementation. It emphasizes key applications of AI in energy

management, transportation, public safety, and healthcare while also addressing vulnerabilities in these domains. The study further identifies a critical gap between advancements in AI and the corresponding focus on cybersecurity, advocating for a balanced approach to innovation.

This research proves the effectiveness of the applied AI and IoT approaches in improving the performance of smart cities, however, the study also highlights the risks that are associated with the application of these technologies. In order to achieve the goal of building secure and inclusive smart cities, the following conclusions are made:

- The discrepancy between the evolution of AI and cybersecurity shows that paying attention to the security aspect of the development process is crucial. It is, therefore, important for AI-driven systems to have strong cybersecurity mechanisms to secure sensitive infrastructure and citizens' information.
- Standard and transparent governance frameworks and ethical guidelines are crucial to addressing issues of data privacy, algorithmic bias, and socio-economic justice. Multi-stakeholder collaboration is, therefore, important in building confidence and sustainable innovation.
- This paper thus presents the need for approaches that are focused on the resilience of the smart city systems because of their interconnectedness and the risks of cascading failures. Tools like digital twins and predictive analytics can help in the risk management and improvement of the urban planning.
- R&D funding in multiple disciplines is crucial to closing the gap between technological progress and its impact on society. This includes developing competence in the areas of cybersecurity, ethical AI, and urban planning and management.
- Solving the multifaceted problems of smart cities needs a collaborative effort of the international community in order to share experiences, harmonize standards, and set international standards for AI and IoT.

Thus, the key areas which require attention in order to enhance the development of smart cities into secure, adaptive and inclusive environments for the future generations are identified. The paper provides a way for actors to manage the risks and seize the opportunities in the digital revolution of urban environments.

REFERENCES

ACHAAL, Batoul et al., 2024. Study of smart grid cyber-security, examining architectures, communication networks, cyber-attacks, countermeasure techniques, and challenges. Cybersecurity. 2 May 2024. Vol. 7, no. 1, p. 10. DOI 10.1186/s42400-023-00200-w.

Artificial Intelligence in Building Management, Bosch Energy and Building Solutions Global. Online. https://www.boschbuildingsolutions.com/xc/en/news-and-stories/smart-buildings/artificial-intelligence-in-building-management/ [Accessed 26 January 2025].

Atlanta city computer network remains hobbled by cyberattack, 2018. AP News. Online. https://apnews.com/general-news-efcf232b7202479e808632557d58774c
[Accessed 26 January 2025].

BRIGHENTE, Alessandro et al., 2024. Security and Privacy of Smart Waste Management Systems: A Cyber–Physical System Perspective. IEEE Internet of Things Journal. March 2024. Vol. 11, no. 5, p. 7309–7324. DOI 10.1109/JIOT.2023.3322532.

Cybersecurity Statistics and Trends [updated 2024], . Online. https://www.varonis.com/blog/cybersecurity-statistics [Accessed 26 January 2025].

Cybersecurity statistics to lose sleep over in 2025, WhatIs. Online. https://www.techtarget.com/whatis/34-Cybersecurity-Statistics-to-Lose-Sleep-Over-in-2020 [Accessed 26 January 2025].

EASTWOOD, Noah, 2025. Millions of households at risk of smart meter snooping. The Telegraph. Online. 14 January 2025. https://www.telegraph.co.uk/money/net-zero/millions-households-smart-meter-snooping/ [Accessed 26 January 2025].

GERRISH, Rachel, 2024. Transportation Companies Face Increasing Cyber Risks. . Online. December 2024. https://www.spglobal.com/ratings/en/research/articles/241212-transportation-companies-face-increasing-cyber-risks-13334611
[Accessed 26 January 2025].

Google Trends for "artificial intelligence" and "cybersecurity," 2025. Google Trends. Online. https://trends.google.com/trends/explore?date=today%205-y&q=artificial%20intelligence,cybersecurity&hl=en [Accessed 25 January 2025].

Groundbreaking Framework for the Safe and Secure Deployment of AI in Critical Infrastructure Unveiled by Department of Homeland Security | Homeland Security, 2024. . Online. https://www.dhs.gov/archive/news/2024/11/14/groundbreaking-framework-safe-and-secure-deployment-ai-critical-infrastructure [Accessed 26 January 2025].

HARRISON, C. et al., 2010. Foundations for Smarter Cities. IBM Journal of Research and Development. July 2010. Vol. 54, no. 4, p. 1–16. DOI 10.1147/JRD.2010.2048257.

HASSANZADEH, Amin et al., 2020. A Review of Cybersecurity Incidents in the Water Sector. Journal of Environmental Engineering. May 2020. Vol. 146, no. 5, p. 03120003. DOI 10.1061/(ASCE)EE.1943-7870.0001686.

HAUGAARD, Annmette, 2020. Smart Waste Management and Increasing Adoption of IoT Solutions. The Smart City Journal. Online. 18 June 2020. https://www.thesmartcityjournal.com/en/articles/smart-waste-management [Accessed 25 January 2025].

HOFER, Florian and RUSSO, Barbara, 2021. Architecture and Its Vulnerabilities in Smart-Lighting Systems. Online. 19 September 2021. arXiv. arXiv:2109.09171. [Accessed 26 January 2025].

IEEE Xplore, . Online. https://ieeexplore.ieee.org/Xplore/home.jsp [Accessed 22 June 2024].

Key Cyber Security Statistics for 2025, SentinelOne. Online. https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-statistics/ [Accessed 26 January 2025].

KIM, Kyounggon et al., 2023. Cybersecurity and Cyber Forensics for Smart Cities: A Comprehensive Literature Review and Survey. Sensors (Basel, Switzerland). 2 April 2023. Vol. 23, no. 7, p. 3681. DOI 10.3390/s23073681.

KONDEPUDI, Sekhar et al., 2014. Smart sustainable cities: an analysis of definitions. Online. https://studylib.net/doc/6879717/smart-sustainable-cities--an-analysis-of-definitions [Accessed 26 January 2025].

LAUFS, Julian et al., 2020. Security and the smart city: A systematic review. Sustainable Cities and Society. 1 April 2020. Vol. 55, p. 102023. DOI 10.1016/j.scs.2020.102023.

LI, Guowen et al., 2023. A critical review of cyber-physical security for building automation systems. Annual Reviews in Control. 2023. Vol. 55, p. 237–254. DOI 10.1016/j.arcontrol.2023.02.004.

LOPES, João, 2024. Virtual Singapore – Singapore's virtual twin - Observatory of Public Sector Innovation. . Online. 5 November 2024. https://oecd-opsi.org/innovations/virtual-twin-singapore/, https://oecd-opsi.org/innovations/virtual-twin-singapore/ [Accessed 25 January 2025].

MECHEVA, Teodora and KAKANAKOV, Nikolay, 2020. Cybersecurity in Intelligent Transportation Systems. Computers. December 2020. Vol. 9, no. 4, p. 83. DOI 10.3390/computers9040083.

NAPHADE, Milind et al., 2011. Smarter Cities and Their Innovation Challenges. Computer. June 2011. Vol. 44, no. 6, p. 32–39. DOI 10.1109/MC.2011.187.

NIST Identifies Types of Cyberattacks That Manipulate Behavior of AI Systems, 2024. NIST. Online. https://www.nist.gov/news-events/news/2024/01/nist-identifies-types-cyberattacks-manipulate-behavior-ai-systems [Accessed 26 January 2025].

NYC Cyber Command - Google AI for Public Sector, Google Public Sector. Online. https://publicsector.google/ai/keeping-new-york-city-digital-services-more-secure-at-massive-scale [Accessed 25 January 2025].

PRANTO, Tahmid et al., 2022. Blockchain and Machine Learning for Fraud Detection A Privacy-Preserving and Adaptive Incentive Based Approach.

ScienceDirect.com | Science, health and medical journals, full text articles and books., . Online. https://www.sciencedirect.com/ [Accessed 22 June 2024].

SEH, Adil Hussain et al., 2020. Healthcare Data Breaches: Insights and Implications. Healthcare. 13 May 2020. Vol. 8, no. 2, p. 133. DOI 10.3390/healthcare8020133.

ŞERBAN, Andreea Claudia and LYTRAS, Miltiadis D., 2020. Artificial Intelligence for Smart Renewable Energy Sector in Europe—Smart Energy Infrastructures for Next Generation Smart Cities. IEEE Access. 2020. Vol. 8, p. 77364–77377. DOI 10.1109/ACCESS.2020.2990123.

VASILEIOU, Ismini, 2020. Cyber Security Education and Training Delivering Industry Relevant Education and Skills via Degree Apprenticeships. In: CLARKE, Nathan and FURNELL, Steven (eds.), Human Aspects of Information Security and Assurance. Cham: Springer International Publishing. 2020. p. 175–185. ISBN 978-3-030-57404-8. DOI 10.1007/978-3-030-57404-8_14.

WOETZEL, Lola et al., 2018. Smart city technology for a more liveable future | McKinsey. Online. https://www.mckinsey.com/capabilities/operations/our-insights/smart-cities-digital-solutions-for-a-more-livable-future [Accessed 29 January 2025].

WOLNIAK, Radosław and STECUŁA, Kinga, 2024. Artificial Intelligence in Smart Cities—Applications, Barriers, and Future Directions: A Review. Smart Cities. June 2024. Vol. 7, no. 3, p. 1346–1389. DOI 10.3390/smartcities7030057.