JOURNAL OF INFORMATION SYSTEMS AND TECHNOLOGY

Journal of Information Systems and Technology
ISSN 3110-4096 (online)
https://athallahpublishing.com/index.php/jaip/index

OPEN ACCESS

Vol. 2, No. 1, 2026

DOI: 10.64845/jistech.v1i2

Towards Adaptive Cybersecurity in Smart Cities: Threat Trends, Mitigation Strategies, and Future Scenarios

Egi Al Fansyah[1*], Muharman Lubis[2], Muhammad Dwi Hary Sandy[3]

[1, 2,3,] *School of Industrial and System Engineering, Telkom University, Indonesia*
Corresponding Author: egialfansyah@student.telkomuniversity.ac.id

ABSTRACT

Smart Cities, which represent modern technology-based urban environments, are currently faced with significant challenges concerning cybersecurity. Cyber threats targeting the digital infrastructure and sensitive data within Smart Cities continue to evolve alongside the increasing levels of connectivity and reliance on technology. Various types of attacks, such as Distributed Denial of Service (DDoS), Ransomware, and exploitation of Internet of Things (IoT) devices, have become threats that warrant serious attention. Therefore, the implementation of effective mitigation strategies is essential to safeguard the security of Smart Cities. This paper examines various potential cyber threats that could jeopardize Smart Cities and evaluates the effectiveness of mitigation strategies that have been implemented, such as the adoption of the Zero Trust model, multi-factor authentication, and real-time anomaly detection systems. Furthermore, this paper discusses recent research developments in threat mitigation technologies, including the utilization of artificial intelligence and blockchain. Findings from this analysis indicate that, in order to ensure the sustainability and security of Smart Cities, more stringent policies, cross-sector collaboration, and ongoing research in mitigation technology development are required.

Keywords: Smart City, Cybersecurity,Threat Mitigation, Trend Analysis, Cyber Threat Intelligence

Received:	Revised:	Accepted:	Available online:
01.10.2025	01.12.2025	01.01.2026	26.02.2026

INTRODUCTION

The rapid development of digital technology in recent decades has given rise to the idea of Smart Cities, namely urban environments that are deliberately designed to improve residents' quality of life through extensive use of digital systems. In this approach, city governments seek higher levels of efficiency and optimization, both in infrastructure management and in the delivery of public services. To support that goal, Smart Cities usually bring together a range of advanced technologies such as Artificial Intelligence (AI), the Internet of Things (IoT), and data analytics that continuously collect, process, and interpret information from many points across the urban space. Put in simpler terms, Smart Cities can be viewed as intelligent cities that rely on technological capabilities to strengthen operational efficiency, encourage sustainable development, and organise public services so that they are more closely aligned with citizens' needs (Almeida, 2023; Kuang et al., 2024)

At the same time, building a city on top of digital infrastructure also creates new vulnerabilities. Systems that are interconnected and always online are exposed to cyberattacks that may interfere with, or even disrupt, the functioning of Smart City services. These risks represent a serious challenge for the safety and security of residents, which means they need to be managed proactively if uninterrupted service provision is to be maintained(Park et al., 2022). Experiences from several cities illustrate how critical such mitigation efforts are. A frequently cited case is the 2018 ransomware attack on the city of Atlanta, where many public services were forced to halt their operations. Other possible threats include distributed denial of service (DDoS) attacks or the hacking of control systems that regulate key public services. Incidents of this type have the potential to undermine both the security and the everyday safety of the urban population(Priyadarshini, 2024).

The advancement of technology has given rise to the concept of Smart Cities, which manage various sectors such as public services, traffic management, transportation, energy, healthcare, and waste management. This concept integrates the Internet of Things (IoT), Artificial Intelligence (AI), and data management to provide both information and automation for public services. The illustration below outlines several key components of Smart Cities. Each component relies on advanced technologies to enable automation, thereby enhancing the efficiency and effectiveness of operations(Houichi et al., 2024). Smart

Cities, comprising various sectors, are supported by digital technologies such as the Internet of Things (IoT), Artificial Intelligence (AI), Big Data, and Blockchain(Alhalafi & Veeraraghavan, 2023; Hossain et al., 2024).

Cybersecurity is a proactive strategy aimed at safeguarding networks, computers, software, and data from attacks, damage, and unauthorized access. According to the National Institute of Standards and Technology (NIST) in the United States, cybersecurity is defined as "the process of protecting information by preventing, detecting, and responding to attacks." Meanwhile, the International Organization for Standardization (ISO) defines cybersecurity as "the preservation of the safety of individuals, organizations, and nations from cyber-related risks." In essence, cybersecurity encompasses a broad set of practices and technologies designed not only to defend digital infrastructure but also to ensure the resilience and trustworthiness of information systems. As digital ecosystems like Smart Cities become increasingly interconnected and data-driven, cybersecurity plays a critical role in maintaining operational continuity, public safety, and the protection of sensitive information from evolving cyber threats(Hossain et al., 2024).

Cyber threats refer to activities intended to undermine or incapacitate network systems and data. In the digital era, the concept of Smart Cities characterized by extensive digitization is particularly vulnerable to potential cyberattacks(Baig et al., 2022; Caivano et al., 2023). Mitigation strategies and risk management for Cyber Smart Cities are essential to ensure the sustained protection of public security within these urban environments. Numerous frameworks are available to anticipate and address the risks posed by cyberattacks. Among them, ISO 31000 stands out as a comprehensive framework offering guidance for the general mitigation of cyber risk(Demertzi et al., 2023). Smart Cities that employ digital technologies such as IoT, AI, and Big Data require comprehensive monitoring of all activity logs. The implementation of Security Incident and Event Management (SIEM) can serve as an effective solution for real-time security monitoring, log activity collection, and correlation analysis to detect suspicious activities within the network systems of Smart Cities(Maheshwari et al., 2024). Furthermore, Cyber Resilience can also be applied to the security systems of Smart Cities. The ability of a system to withstand, respond to, and recover from cyberattacks without disruption over the long term is a critical capability

required to maintain the integrity and continuity of security networks within Smart Cities(Tan, 2024).

The majority of mitigation strategies currently employed are reactive and focused on post-attack responses, without taking into account the evolving dynamics of future threats. Such an approach is inadequate in the context of Smart Cities, which are complex, adaptive, and constantly changing. The limited use of foresight techniques in designing security strategies results in insufficient preparedness of systems against unidentified attacks(Bauer et al., 2021). To address these challenges, this study aims to develop a security mitigation framework for Smart Cities based on a foresight techniques approach, such as trend analysis and scenario planning. This framework is expected to provide more advanced, proactive, and relevant mitigation solutions in response to the evolving dynamics of future cyber threats. This study aims to address two main questions: (1) What are the most effective and efficient mitigation strategies in dealing with various potential threats to Smart Cities? and (2) How can future research and technology trends shape more adaptive mitigation strategies against cyberattacks?

The main contributions of this study include a synthesis of recent literature on security challenges in Smart Cities, the identification of technological trends and future threat scenarios, and the development of a conceptual mitigation framework based on foresight(Wepner et al., 2025). This article is organized into several sections, beginning with a literature review, followed by the research methodology, the results and discussion of the developed framework, and concluding with conclusions and recommendations for future research. This article will focus on describing several mitigation strategies that can be implemented in the event of an attack on Smart Cities. In addition, it will categorize potential cyberattacks that may occur in Smart Cities and identify the possible threats they may face.

METHOD

The study on “Cyber Threats to Smart Cities and Their Mitigation Strategies” employs a foresight approach to identify current and emerging cybersecurity trends within the Smart City ecosystem(Bauer et al., 2021; Wepner et al., 2025). The primary focus of applying this methodology is to analyze technological dynamics and formulate

strategic scenarios that can serve as a foundation for designing security mitigation measures. The primary focus of applying this methodology is to analyze technological dynamics and formulate strategic scenarios that can serve as a foundation for designing security mitigation measures.

Trend analysis was conducted by searching literature across various scientific databases. However, in this study, the literature search was specifically focused on the Scopus database. The literature was utilized to identify key factors within the domain of Smart City security, such as identification of cyber threats, proposed mitigation strategies, advantages and limitation and directions for future research

Figure 1. Research Flow

The research flow, as illustrated in Figure 1, begins with the identification of problems within the study to uncover issues or phenomena occurring in the Smart Cities security ecosystem. This is followed by the establishment of research objectives, which serve to define the scope of the study and focus on the key issues to be addressed. Subsequently, the identification of security threats aims to categorize the various types of threats encountered. The mitigation strategies gathered from diverse literature sources help to determine the strengths and

weaknesses of each proposed method. Additionally, the advantages and limitations of each relevant literature piece concerning Smart Cities security systems are analyzed. Finally, the study explores future research trends in threat mitigation, which will guide the development of mitigation plans for the ongoing evolution of the Smart Cities ecosystem. Based on the identified trends, this study will develop several future scenarios by considering two key uncertainties. The level of connectivity and technological complexity and the maturity of security policies and regulations

RESULTS

This section presents the key findings from the literature review on cybersecurity threats faced by Smart Cities, along with the mitigation strategies that have been proposed. It further discusses the strengths and limitations of the various mitigation approaches identified, followed by an exploration of potential future research directions aimed at developing more adaptive and sustainable security solutions.

Identification of Security Threats in Smart Cities

Based on the review of several pieces of literature, it was found that the Smart City ecosystem faces various types of cyber threats.

1. *Advanced Persistent Threats (APT)*: It is considered one of the most dangerous types of attacks, as it systematically targets the city's vital infrastructure in a covert manner and over an extended period. Advanced Persistent Threats (APTs) are typically carried out by highly capable actors, potentially involving state-sponsored entities, with the objective of gaining control over critical systems such as power grids, water supply networks, or intelligent transportation systems.
2. *Vulnerabilities in IoT Communication*: This represents a serious vulnerability that allows attackers to infiltrate the city's network and gain unauthorized access to control systems. Given the massive and widespread deployment of IoT devices, even the smallest security gap can be exploited to launch large-scale attacks, including Distributed Denial of Service (DDoS) attacks and the takeover of control systems.
3. *Weaknesses in Authentication and Encryption Systems*: in edge devices and city sensors also create opportunities for the interception and manipulation of critical data. This issue is further exacerbated by the

limited computational resources of these devices, which hinder the implementation of more robust security schemes.

4. *Lack of User Security Awareness*: In particular, the low level of security awareness and digital literacy among users and system operators adds to the complexity of the threat landscape. Social engineering techniques, such as phishing or psychological manipulation to remain effective methods for attackers to gain access without having to breach complex technical systems.

Overall, these findings underscore the urgency that security mitigation efforts in Smart Cities cannot be solely focused on strengthening technical or hardware aspects. Instead, a holistic approach is required—one that also encompasses policy development, risk management, digital security governance, and the enhancement of human capacity and awareness as integral components of the smart city ecosystem.

Proposed Mitigation Strategies

From the review of various literature, it was found that numerous mitigation approaches have been extensively discussed to address cyber threats within the Smart City environment. These approaches emphasize the importance of a more proactive, integrated, and predictive response to increasingly dynamic attack patterns. *Cyber Threat Intelligence (CTI)*: A cybersecurity intelligence system that actively collects, analyses and disseminates information related to potential threats and the latest attack techniques. Supported by Cyber Threat Intelligence (CTI), Smart City security systems can detect early signs of attacks, map attack patterns based on both historical and real-time data, and respond swiftly to prevent more significant impacts. *Intrusion Detection System (IDS)*: Machine learning algorithms have emerged as a rapidly advancing solution. These systems are designed to detect anomalies in network traffic that deviate from normal behaviour. The advantage of machine learning-based Intrusion Detection Systems (IDS) lies in their ability to adaptively learn data patterns, enabling the identification of novel attacks that traditional signature-based systems may fail to recognize.

External Audit-*Based Risk Management*: This approach emphasizes the importance of periodic security evaluations conducted by independent third parties. Such audits encompass not only technical aspects, including system configurations and network resilience, but also

administrative dimensions such as policies, processes, and compliance with information security standards. *Adaptive Security Framework*: The system automatically adjusts to the level of threat, resource availability, and operational environment. However, it is important to note that the design architecture of this adaptive framework remains largely conceptual, with few concrete implementations or prototypes available for direct testing.

From the comprehensive approaches reviewed, it is evident that a combination of proactive detection technologies and robust data protection policies constitutes the most promising mitigation strategy. The synergy between technical capabilities for automatic attack recognition and a policy framework that supports rapid, coordinated response is key to establishing a resilient and sustainable Smart City security system.

Table 1. Comparison of Threats and Solutions

Type of Threats	Mitigation Solutions	Advantages	Limitations	Citation
Advanced Persistent Threats (APT)	Cyber Threat Intelligence (CTI) for Long-Term Pattern Detection	Effective for detecting covert and complex attacks	Requires data integration and regular intelligence updates	(Achuthan et al., 2025; Alhalafi & Veeraraghavan, 2023; Fang et al., 2025; Houichi et al., 2024)

Type of Threats	Mitigation Solutions	Advantages	Limitations	Citation
Device and IoT Vulnerabilities	Machine Learning-Based Intrusion Detection System (IDS) for Anomaly Monitoring	Capable of learning and adapting to new patterns	Prone to false positives; requires tuning and extensive data training	(Almeida, 2023; Baig et al., 2022; Degtereva et al., 2020; Houichi et al., 2024; Padmashree & Krishnamoorthi, 2022)
Data Manipulation / Weak Encryption	Strengthening security protocols and implementing advanced encryption techniques	Provides fundamental protection across all communication levels	Requires high computational power and compatibility	(Achuthan et al., 2025; Almeida, 2023; Degtereva et al., 2020; Leroy et al., 2025)
Lack of Security Awareness	Cybersecurity training and awareness programs for users and operators	Enhances defenses based on human behavior	Challenging to implement without policy support	(Demertzi et al., 2023; Hossain et al., 2024; Houichi et al., 2024; Kuang et al., 2024)

Type of Threats	Mitigation Solutions	Advantages	Limitations	Citation
DDoS / Flooding Attacks	Load balancing, dynamic firewalls, and automated response systems	Prevents system overload and minimizes downtime	Less effective against stealthy or multilayered attacks	(Alhalafi & Veeraraghavan, 2023; Caivano et al., 2023; Kuang et al., 2024; Leroy et al., 2025; Priyadarshini, 2024)

(Source: Primary Data, Processing 2025)

In addition to the descriptive explanations of threat types and mitigation approaches found in the literature, Table 1 below presents a comparative summary of the main cyber threats within the Smart City context alongside recommended mitigation solutions. This table also highlights the advantages and limitations of each solution, providing a comprehensive overview of the effectiveness and challenges associated with implementing these mitigation strategies. For example, Advanced Persistent Threats (APT), which are covert and target critical infrastructure over an extended period, require an approach based on Cyber Threat Intelligence (CTI). CTI is considered effective because it can detect attack patterns at an early stage; however, its success heavily depends on the availability of real-time data and robust integration of intelligence systems. On the other hand, threats arising from IoT device vulnerabilities, such as gaps in inter-device communication, are more suitably addressed through machine learning-based Intrusion Detection Systems (IDS). IDS enable the detection of anomalies in network traffic but still carries the risk of false positives, which must be mitigated through proper model tuning and training.

Some solutions also address non-technical dimensions, such as cybersecurity training and awareness programs, which are crucial in combating social engineering-based attacks. Unfortunately, this aspect is often overlooked in the design of urban technology systems. Other technical approaches, such as strengthening encryption protocols or

utilizing dynamic firewalls, also have limitations depending on the implementation environment. Overall, this table underscores that no single solution can address all types of threats. Therefore, an ideal Smart City security mitigation strategy should be multi-layered and integrative, encompassing technological aspects, governance, and human resources.

Discussion

Analysis of Strengths and Limitations

From the analysis of the reviewed literature, it is evident that most studies concur on the insufficiency of conventional approaches to addressing cyberattacks within Smart City environments. The increasingly sophisticated, stealthy, and adaptive nature of these threats necessitates mitigation strategies that are multi-layered, responsive, and grounded in current data and context. For instance, Cyber Threat Intelligence (CTI) is deemed highly effective in managing Advanced Persistent Threat (APT) type attacks due to its capability to identify attack patterns and recommend actions before significant incidents occur. Nevertheless, the efficacy of CTI is highly contingent upon the availability of comprehensive real-time data, and it demands robust technological infrastructure support and analytical systems capable of handling significant data complexity.

Meanwhile, Machine Learning-based Intrusion Detection Systems (IDS) are recognized for their high accuracy in detecting suspicious activities within network traffic. However, these systems still contend with the significant challenge of high false positive rates, which can lead to operational disruptions or alert fatigue for security teams. From a non-technical standpoint, approaches centered on enhancing cybersecurity awareness and training represent a crucial aspect often overlooked in the prioritization of Smart City system development. This is despite the fact that human factors frequently serve as the primary entry point for social engineering attacks. The low security literacy among users, operators, and policymakers further exacerbates the complexity of risks, which cannot be mitigated solely through technical solutions.

Overall, this analysis reinforces the argument that optimal mitigation in the Smart City context must be multi-layered, not solely reliant on technology. Instead, it must also encompass the strengthening of regulations, the formulation of adaptive security policies, the enhancement of human resource capacity, and collaboration among

stakeholders. This integrated approach is crucial to ensure that security systems are not only robust against current threats but also capable of adapting to the dynamics of future risks.

Future Research Directions

Based on the analysis of the reviewed literature, it is evident that the majority of studies concur that conventional approaches to addressing cyberattacks in Smart City environments are no longer sufficiently effective. The increasingly sophisticated, covert, and adaptive nature of threats necessitates a multi-layered, responsive mitigation strategy that is grounded in current data and contextual awareness. *Anomaly detection in IoT will become a primary focus:* In the future, anomaly detection in IoT is expected to become a central focus of upcoming research. As IoT devices become increasingly dominant across various Smart City sectors—such as transportation, lighting, water systems, and public security—the ability to detect abnormal behavior in real time will be crucial for preventing systemic disruptions. The main challenges in this regard include the limited processing power of edge devices and the diversity of communication standards employed.

The Utilization of Deep Learning: Predicting and classifying cyberattacks with greater accuracy. Compared to traditional machine learning approaches, deep learning is capable of capturing complex patterns within continuously evolving large datasets. However, the accompanying challenges include the high computational demands and the necessity for representative and secure datasets. *Integration of foresight and threat trend mapping*: In this manner, the system is designed not only to counter currently known threats but also to be prepared to respond to emergent and yet explicitly undocumented threats. This approach aligns with the principle of "future-proofing," which is increasingly being adopted in smart city planning. *Expansion of the adaptive framework*: A flexible framework that can be tailored to specific domain contexts is required. For instance, security needs in the smart transportation sector differ significantly from those in e-health systems or smart electrical grids. Therefore, mitigation models must be designed to be modular and adaptive, allowing implementation according to the unique requirements of each sector without compromising architectural cohesion

CONCLUSION

Smart City, as a form of digitally-driven urban transformation, presents numerous opportunities to enhance the efficiency of public services and leverage advanced technologies. However, alongside the high level of technological integration, significant challenges arise in safeguarding against cyber threats. This study highlights that reactive and traditional security approaches are no longer adequate to address complex threats such as Advanced Persistent Threats (APT), IoT device exploitation, data manipulation, and the low awareness of users regarding digital security. By adopting a foresight approach through trend analysis and future scenario development, this research designs a comprehensive mitigation framework. This framework not only relies on technology as the primary solution but also incorporates policy considerations, regulatory measures, and the enhancement of human resource capabilities. The proposed mitigation strategy is multi-layered, encompassing adaptive detection technologies, predictive approaches, and policy support that is responsive to the evolving threat landscape. The conclusions of this study affirm that creating a secure and sustainable Smart City requires intersectoral synergy, robust policy formulation, and the strengthening of continuous research focused on the development of anticipatory and scenario-based long-term security systems.

REFERENCES

Achuthan, K., Sankaran, S., Roy, S., & Raman, R. (2025). Integrating sustainability into cybersecurity: insights from machine learning based topic modeling. *Discover Sustainability*, *6*(1). https://doi.org/10.1007/s43621-024-00754-w

Alhalafi, N., & Veeraraghavan, P. (2023). Exploring the Challenges and Issues in Adopting Cybersecurity in Saudi Smart Cities: Conceptualization of the Cybersecurity-Based UTAUT Model. *Smart Cities*, *6*(3), 1523–1544. https://doi.org/10.3390/smartcities6030072

Almeida, F. (2023). Prospects of Cybersecurity in Smart Cities. *Future Internet*, *15*(9). https://doi.org/10.3390/fi15090285

Baig, Z., Syed, N., & Mohammad, N. (2022). Securing the Smart City Airspace: Drone Cyber Attack Detection through Machine Learning. *Future Internet*, *14*(7). https://doi.org/10.3390/fi14070205

Bauer, J., Konrad, C., Hechtel, M., Wichert, R., Weigand, C., Dengler, S., Holzwarth, M., & Franke, J. (2021). ForeSight Approach to improve Privacy and Security in the Smart Living Domain. *Current Directions in Biomedical Engineering*, *7*(2), 903 – 906. https://doi.org/10.1515/cdbme-2021-2230

Caivano, D., De Vincentiis, M., Pal, A., & Ragone, A. (2023). Securing Smart Cities: Unraveling Quantum as a Service. *QP4SE 2023 - Proceedings of the 2nd International Workshop on Quantum Programming for Software Engineering, Co-Located with: ESEC/FSE 2023*, 1–6. https://doi.org/10.1145/3617570.3617865

Degtereva, V., Gladkova, S., Makarova, O., & Melkostupov, E. (2020, November 18). Forming a Mechanism for Preventing the Violations in Cyberspace at the Time of Digitalization: Common cyber threats and ways to escape them. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3446434.3446468

Demertzi, V., Demertzis, S., & Demertzis, K. (2023). An Overview of Cyber Threats, Attacks and Countermeasures on the Primary Domains of Smart Cities. In *Applied Sciences (Switzerland)* (Vol. 13, Issue 2). MDPI. https://doi.org/10.3390/app13020790

Fang, J., Tang, Y., & Guo, M. (2025). Comprehensive Review of Cyber Threat Intelligence Sharing: Challenges and Methodologies. *Proceedings of the 4th Asia-Pacific Artificial Intelligence and Big Data Forum, AIBDF 2024*, 455–461. https://doi.org/10.1145/3718491.3718565

Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2024). Local Government Cybersecurity Landscape: A Systematic Review and Conceptual Framework. In *Applied Sciences (Switzerland)* (Vol. 14, Issue 13). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/app14135501

Houichi, M., Jaidi, F., & Bouhoula, A. (2024). A comprehensive and in-depth study of the threats faced by smart cities and the countermeasures implemented in their key areas. *Journal of Infrastructure, Policy and Development*, *8*(10). https://doi.org/10.24294/jipd.v8i10.8629

Kuang, Z., Su, J., Latifian, A., Eshraghi, S., & Ghafari, A. (2024). Utilizing Artificial neural networks (ANN) to regulate Smart cities for sustainable Urban Development and Safeguarding Citizen rights. *Scientific Reports*, *14*(1). https://doi.org/10.1038/s41598-024-76964

Leroy, I., Zolotaryova, I., & Semenov, S. (2025). Impact of Critical Infrastructure Cyber Security on the Sustainable Development of Smart Cities: Insights from Internal Specialists and External Information Security Auditors. *Sustainability (Switzerland)*, *17*(3). https://doi.org/10.3390/su17031188

Maheshwari, R. U., Shankar, P. R., Chandrasekaran, G., & Mahendrakhan, K. (2024). Assessment of Cybersecurity Risks in Digital Twin Deployments in Smart Cities. *International Journal of Computational and Experimental Science and Engineering*, *10*(4), 695–700. https://doi.org/10.22399/ijcesen.494

Padmashree, A., & Krishnamoorthi, M. (2022). Decision Tree with Pearson Correlation-based Recursive Feature Elimination Model for Attack Detection in IoT Environment. *Information Technology and Control*, *51*(4), 771–785. https://doi.org/10.5755/j01.itc.51.4.31818

Park, J. H., Singh, S. K., Salim, M. M., Azzaoui, A. E. L., & Park, J. H. (2022). Ransomware-based Cyber Attacks: A Comprehensive Survey. *Journal of Internet Technology*, *23*(7), 1557–1564. https://doi.org/10.53106/160792642022122307010

Priyadarshini, I. (2024). Anomaly Detection of IoT Cyberattacks in Smart Cities Using Federated Learning and Split Learning. *Big Data and Cognitive Computing*, *8*(3). https://doi.org/10.3390/bdcc8030021

Tan, C. (2024). Response Strategies to Cyber Threats in Service Industries. *ACM International Conference Proceeding Series*, 203–207. https://doi.org/10.1145/3700906.3700939

Wepner, B., Neuberger, S., Hörlesberger, M., Molin, E. M., Lampert, J., & Koch, H. (2025). How can digitalisation support transformation towards sustainable agri-food systems? Scenario development in Lower Austria. *Agricultural Systems*, *224*. https://doi.org/10.1016/j.agsy.2024.104251