JSIP: Jurnal Studi Ilmu Pemerintahan
Volume 4, No 2,2023
ISSN: 2722-7405

Research Trends, Topics, and Insights on Network Security and the Internet of Things in Smart Cities

Velandani Prakoso*[1], Herman Lawelai [2], Achmad Nurmandi[2],
Eko Priyo Purnomo[2], Hazel Jovita[3]

[1]*Department of Information Systems, Universitas Siber Muhammadiyah, Indonesia*
[2]*Doctoral Program of Government Affairs and Administration, Jusuf Kalla School of Government, Universitas Muhammadiyah Yogyakarta, Indonesia*
[3]*Department of Political Science, Mindanao State University-Iligan Institute of Technology, Philippines*

Co-Authors: velandani@sibermu.ac.id

Article Info

Keyword:
Network Security,
Internet of Things,
Smart City,
Cyberthreats,
Sustainability,

Abstract: This research investigates network security and the Internet of Things in smart cities, focusing on their vulnerability to cyber threats due to advanced technologies and widespread connectivity. The aim is to address current security challenges and develop a security vision for a sustainable smart city future. The research method involves bibliometric analysis of 517 documents from the Scopus database using the VOSviewer analysis tool and CiteSpace for network visualization analysis. The findings show increased research on network security and IoT in smart cities, focusing on operational sustainability and data security. Integrating technologies like big data, artificial intelligence, and machine learning is crucial in addressing these complex challenges. The research emphasizes the importance of network security in maintaining data integrity and confidentiality in smart cities and the integration of IoT technologies in decision-making. Recommendations include developing advanced security techniques, integrating big data and sustainability, crisis monitoring, and blockchain exploration. Further research is expected to improve network security and IoT implementation, contributing to efficiency, convenience, and quality of life in an increasingly connected urban society.

Article History:
Received: 12 March 2023
Revision: 29 Juni 2023
Accepted: 20 Agustus 2023

DOI: https://doi.org/10.35326/jsip.v4i2.4707

INTRODUCTION

In this era of fast-paced technology (Gyamfi et al., 2022; Zimand-Sheiner & Lahav, 2022), network security and the Internet of Things (IoT) have become crucial to the smart city concept (Atitallah et al., 2022; Choudhary & Meena, 2022; Elahi et al., 2022; Farooq et al., 2022; Javed et al., 2022). These cities integrate information technology to enhance residents' quality of life, necessitating a sophisticated and responsive security system (Lee-Geiller & Lee, 2019; Parasol, 2018). Network security is essential for the entire infrastructure, as interconnected smart devices, sensors, and automation systems pose security risks (Javed et al., 2022; Kashef et al., 2021). IoT plays a central role in shaping city intelligence and poses significant security risks. It is crucial to protect data and maintain system integrity for the city to function properly.

Stakeholders in smart city development must collaborate to design a comprehensive security solution (Axelsson & Granath, 2018), including encryption technology, real-time security monitoring, and strict security policies (Parasol, 2018). Public education on cyber security practices is also crucial to raise awareness of potential risks (Wirtz et al., 2022). By maintaining secure networks and IoT, smart cities can reach their full potential as efficient, innovative environments. Robust security initiatives will help establish a stable

foundation for the sustainable growth and success of the smart city concept in this era (Hoffman, 2021).

The IoT has revolutionized urban life by enabling the collection and processing of data from sensors and connected devices (Zhang, Pee, Pan, & Cui, 2022), enhancing efficiency, reducing costs, and improving quality of life (Kashef et al., 2021). However, this technology also presents significant security challenges, as the interconnectedness of systems and devices exposes them to potential threats (Okitasari & Katramiz, 2022). Inadequate security can compromise citizens' privacy and increase the risk of cyberattacks, leading to a complete shutdown of city operations (S. E. A. Ali et al., 2021).

To address these issues, robust security protocols must be implemented, including data encryption, authentication, and continuous network monitoring (Imghoure et al., 2022). Involving security experts in planning and implementing IoT systems is crucial to protecting urban infrastructure (Braga et al., 2021). Educating the public about security risks is also essential to protect themselves (O. Ali et al., 2020). By prioritizing security in IoT development and deployment, cities can realize the benefits of these technologies without exposing them to adverse security risks, promoting sustainability and community well-being (Javed et al., 2022).

Developing a network security and IoT strategy for smart cities requires a balance between sustainability, ethical use of technology, and data responsibility (Lee-Geiller & Lee, 2019; Liu et al., 2022). Sustainability is crucial for long-term security solutions, requiring system updates, personnel training, and collaboration with relevant parties (Gkioulos & Chowdhury, 2021). Ethical aspects of technology use include protecting individual privacy and transparency in data management, recognizing citizens' right to keep their personal information private, and providing adequate information on data collection, use, and storage. Strict privacy policies and clear communication efforts can build public trust in smart city initiatives (Mantelero & Esposito, 2021; Peron et al., 2021).

Data responsibility is a key focus, preventing misuse and leakage of information (Ahanger et al., 2022). Strong encryption, careful security monitoring, and clear policies regarding data use (Kimani et al., 2019), and sharing with third parties are essential (Bader et al., 2021). Proactively identifying security risks, preventive measures, and quick responses to threats are crucial (Franchina et al., 2021). This holistic approach ensures effective protection while maintaining sustainability, ethics, and data responsibility in line with societal values and global norms.

Recent literature on network security and the IoT has highlighted the complexity of cyberattacks on smart cities, which pose a significant threat to community sustainability and security (Ashraf et al., 2021; Parasol, 2018). Cyberattacks can disrupt public transportation systems, damage critical infrastructure, and leak citizens' personal information due to the large amount of data generated by smart city infrastructure (Benyahya et al., 2022).

Previous studies have identified weaknesses in security systems, such as inadequate encryption on inter-device communications and hardware weaknesses, which ill-intentioned parties can exploit (Davis, 2022). Robust authentication mechanisms are also needed, as smart cities are tightly connected to various devices, making strong identity and access protection crucial (Afaq et al., 2021; Firouzi et al., 2022; Seyhan & Akleylek, 2022). The complexity of security challenges faced by smart cities necessitates the development of holistic security policies (Khan et al., 2017; Riahi Sfar et al., 2018; Sandeepa et al., 2022), and advanced security technologies to maintain sustainability and

security in the context of smart city development (Li et al., 2022; Zhang, Pee, Pan, & Liu, 2022).

The rapid growth in network security and the IoT has highlighted the need for further research in smart city environments. However, significant knowledge gaps still need to be addressed, particularly in understanding emerging security trends in modern smart cities. With numerous connected devices in urban environments, unique security risks and challenges can arise, necessitating further investigation.

More detailed research on network and IoT security topics in smart cities is also needed, including identifying potential vulnerabilities and developing effective security strategies against rapidly evolving threats. By deepening our knowledge, we can improve system security in smart cities and address future challenges. Continued research in this area is crucial, and researchers are expected to actively contribute to filling this knowledge gap to ensure safe and sustainable development in smart cities.

This research focuses on network security and IoT in smart cities, as they are becoming increasingly vulnerable to cyber threats due to advanced technologies and widespread connectivity. The importance of protecting smart city infrastructure extends beyond technical aspects to the security of citizens and the smooth operation of the entire system. The research aims to address current security challenges and embrace a security vision for a sustainable smart city future.

By engaging with current trends and topics related to network security and IoT, the research seeks to explore deep insights into dealing with dynamic changes in cyber threats in smart city environments. Preventive measures and adaptation strategies are needed to maintain the sustainability and efficiency of smart cities in the long run. The research provides an in-depth understanding of current security challenges in smart cities. It aims to formulate a robust and sustainable view of the future, focusing on innovative, proactive, and holistic solutions.

RESEARCH METHOD

The research uses the Scopus database, a reputable information resource with over 70 million sources covering social sciences (Huo et al., 2022), engineering, computer science, energy, environmental science and arts and humanities (Ennas & Di Guardo, 2015; Montoya et al., 2018; Sánchez-Gil et al., 2018). Scopus is considered a more comprehensive data source than Web of Science and MedLine, which is strongly associated with academic activity (Stapleton et al., 2020). The study adopted the PRISMA method to search for relevant literature on network security and IoT in smart cities.

The findings form the basis for further exploration of the relationship between these two aspects in smart city environments. Scopus was chosen due to its broader topics and multidisciplinary coverage (Martín-Martín et al., 2018). The findings offer insights into network security and IoT in smart cities and serve as a foundation for further research. They can help understand the challenges and opportunities associated with security integration in smart city environments. This research contributes to existing literature and is a foundation for future network and IoT security-related policies and practices.

The search string in Scopus is: ARTICLE TITLE, ABSTRACT, KEYWORDS: "Network Security", "Internet of Things", AND smart city PUBYEAR > 2012 AND PUBYEAR < 2023, LIMIT-TO: SUBJAREA: "SOCI", SOURCE TYPE: "j", and LANGUAGE: "English" The bibliometric analysis involved selecting 517 documents to create a bibliometric map using the VOSviewer analysis tool. This tool provided in-depth insights into the network of relevant literature (Syahputra et al., 2023), allowing researchers to identify trends

(Nurmandi et al., 2021), patterns, and relationships among the selected documents (Lawelai et al., 2023). CiteSpace was used for further analysis of network visualizations, facilitating further assessment of research keyword variables (Chen, 2017; Chen & Song, 2019).

The study used bibliometric analysis tools VOSviewer and CiteSpace to understand the structure, trends, and relationships between relevant documents. VOSviewer visualized the literature network (Barbosa, 2021; Chanduví et al., 2015), while CiteSpace provided a more in-depth analysis of research keywords (Goerlandt et al., 2022). The data processing stage involved document selection, visualization, and analysis of research keywords. However, limitations include the selection of documents based on keywords and databases, which may limit the scope of literature, and potential biases in data processing, which could affect the overall representation of the existing literature network. Co-occurrence analysis and specific topics may not cover all relevant aspects of the complex relationship (Crible & Degand, 2021).

The literature selection process was detailed in a modified PRISMA chart, illustrating the steps taken in searching, selecting, and collecting documents for the analysis. The modifications were tailored to the study's specific needs and depicted visually in Figure 1.

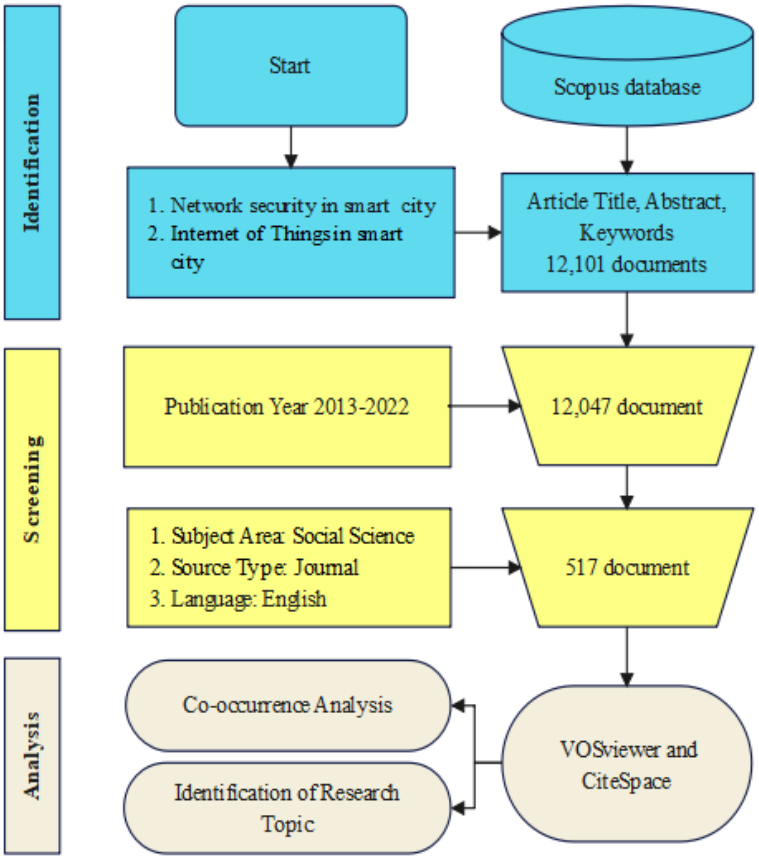

Figure 1. PRISMA chart of literature search and screening

RESULTS AND DISCUSSION

Co-occurrence Analysis

The study explores the relationship between network security and IoT in smart city development, focusing on the application of technology to enhance efficiency, safety, and convenience. It uses co-occurrence analysis to identify patterns in related literature, highlighting the growing importance of these technologies in the digital era.

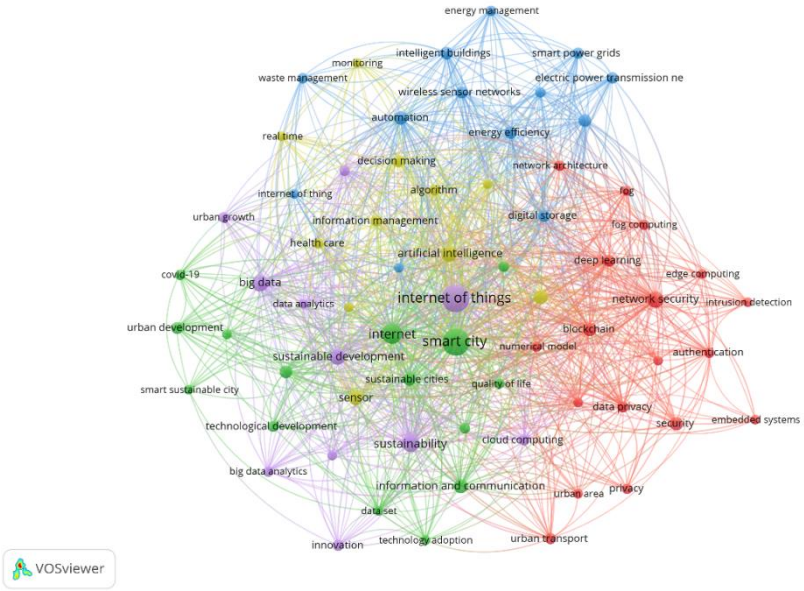

Figure 2. Keyword Co-occurrence Research

Research on network security and Internet of Things (IoT) integration in smart cities reflects the rapid evolution of technological development. In Figure 2 and Table 1, the 20 most frequently occurring key terms highlight the main focus of research on IoT technology integration in smart city environments. In Figure 3, a timeline visualization depicts the development and evolution of keywords in each cluster over time, providing a clear visual picture of keyword dynamics and shifts in focus within a given cluster.

Table 1. Top 20 Keyword Co-occurrence Research

Keyword	Occurrences	Per. (%)	Keyword	Occurrences	Per. (%)
internet of things	295	7,4	sensor	32	0,8
smart city	289	7,2	automation	27	0,7
internet	107	2,7	blockchain	27	0,7
sustainability	69	1,7	security	27	0,7
network security	55	1,4	sustainable cities	24	0,6
big data	53	1,3	urban planning	24	0,6
sustainable development	50	1,2	energy efficiency	22	0,5
artificial intelligence	45	1,1	energy utilization	22	0,5
machine learning	35	0,9	intelligent buildings	22	0,5
ict	32	0,8	decision making	21	0,5

The high number of smart cities confirms that the research involves a deep understanding of how technology can improve cities' overall functioning. Network security is a significant concern in this context, indicating that researchers are considering the risks and challenges associated with implementing IoT technologies in urban environments.

Furthermore, sustainability and development reflect research awareness of environmental impacts and sustainability in smart city development (Khan et al., 2017). The focus on sustainability can also be seen from the occurrence of energy efficiency and utilization, indicating that this research focuses on security and the efficient use of energy resources (Franchina et al., 2021).

The importance of data analysis is evident from big data, artificial intelligence (AI) (Djen et al., 2023), and machine learning, indicating that researchers are exploring how to manage and analyze the large amount of data generated by IoT devices in smart cities. The importance of security and data protection is reflected in security and network security (Javed et al., 2022; Kashef et al., 2021), emphasizing the need to protect infrastructure and data from potential threats.

In addition, the research also includes the concepts of automation, blockchain, sensors, and intelligent buildings, indicating that automation, blockchain technology, sensors, and smart buildings are crucial elements in the development of safe and sustainable smart cities. In this context, urban planning and sustainable cities highlight the importance of integrated and sustainable urban planning to achieve the vision of safe and efficient smart cities. Finally, the occurrence of decision-making shows that this research also considers how decision-making can be optimized using IoT technology and network security.

The research clusters on network security and iot in smart cities are "cloud computing environment," "covert channels," and "e-governance system," as shown in Figure 3. Cloud computing is essential for implementing, managing, and securing IoT infrastructure in smart cities. The covert channel cluster focuses on network security, applying machine learning technology to detect and prevent Denial of Service (DoS) attacks and risks (Hoffman, 2021). The cluster focuses on developing network security methods involving new machine-based approaches to deal with covert attacks and complex cyber threats (Wirtz et al., 2022). The e-governance systems cluster emphasizes the role of Blockchain in improving security, data privacy, and information management in e-governance. Data security and privacy are essential in developing e-governance systems in smart cities (Mantelero & Esposito, 2021). By examining these clusters, this research offers a comprehensive understanding of the vital aspects of Network Security and IoT in Smart Cities, highlighting the frameworks and innovative solutions needed for a sustainable future.

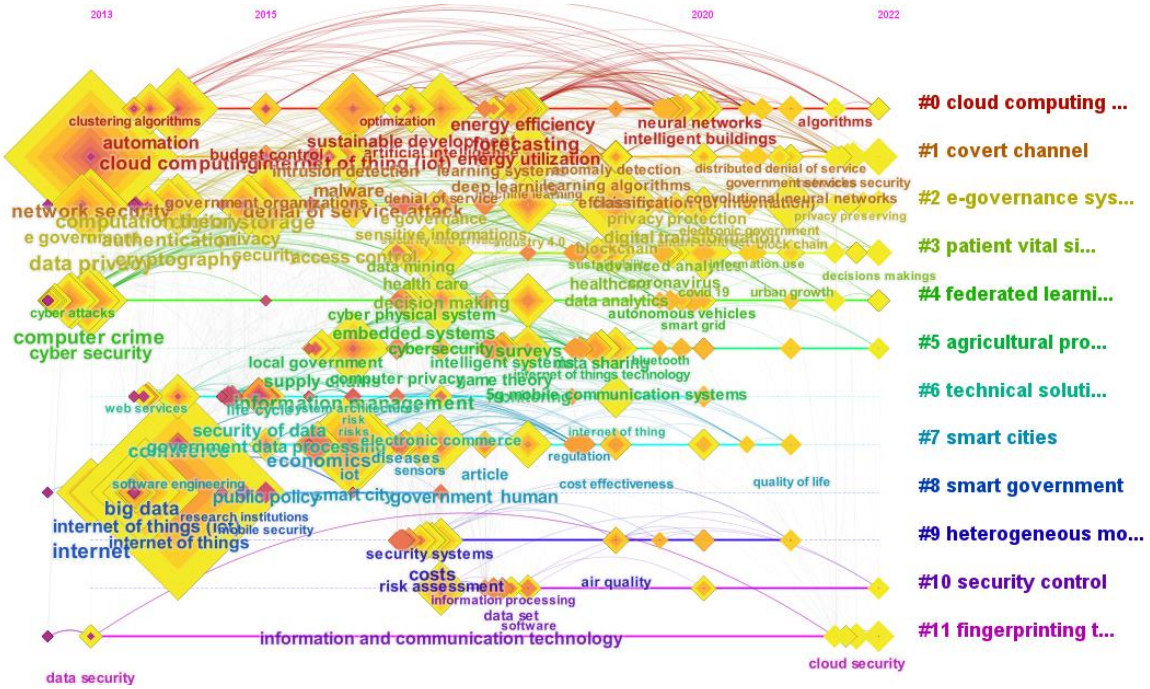

Figure 3. Timeline view of keyword occurrences

Figure 4 displays a visualization of the citation boom period, with a red line indicating the start year and the right end indicating the end year. A blue line reflects the citation timeline, with a light blue line indicating unpublished literature and a dark blue line indicating the publication year. The dark blue part indicates that the keyword was cited between 2013 and 2022. The visualization provides a clear picture of the citation boom period, publication time, and the most significant citation year range.

Keywords	Year	Strength	Begin	End	2013 - 2022
network security	2013	6.52	**2013**	2016	
internet	2013	5.6	**2013**	2016	
computer crime	2013	3.96	**2013**	2018	
data privacy	2013	3.64	**2013**	2018	
software engineering	2014	3.21	**2014**	2017	
government data processing	2015	5.67	**2015**	2017	
security of data	2015	3.87	**2015**	2017	
e governments	2015	2.56	**2015**	2016	
distributed computer systems	2016	6.73	**2016**	2017	
malware	2016	3.1	**2016**	2019	
industrial internet of things	2018	2.77	**2018**	2019	
intelligent systems	2018	2.69	**2018**	2020	
internet of thing (iot)	2016	4.28	**2019**	2022	
5g	2019	2.61	**2019**	2020	
advanced analytics	2020	2.66	**2020**	2022	
data analytics	2019	2.61	**2020**	2022	
government agency	2018	2.55	**2020**	2022	
covid 19	2020	2.52	**2020**	2022	

Figure 4. Top 18 keywords with the strongest citation burst

The Topic of Network Security in Smart Cities

The keyword co-occurrence overlay visualization in Figure 5 shows the relationship of network security in smart cities over time. The color intensity of the overlay network indicates the level of publication, with darker colors indicating older publications and lighter yellowish colors indicating more recent research. These visualizations help identify critical trends, essential points in research history, and areas that need further attention.

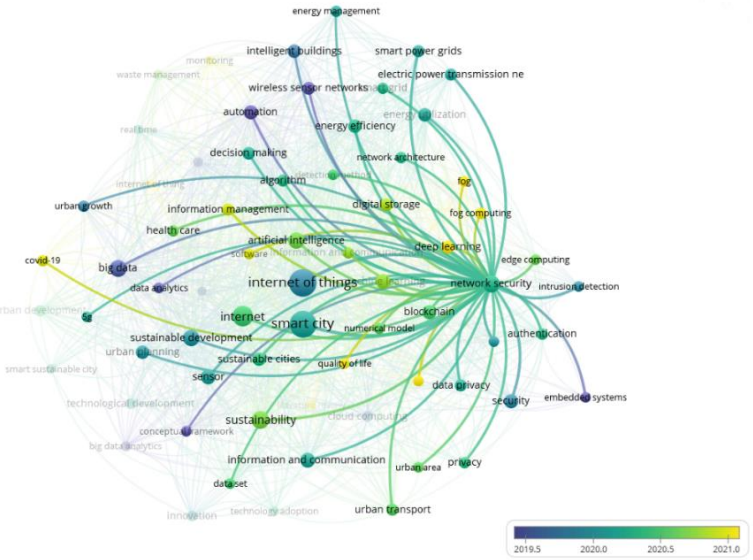

Figure 5. Relationship keyword of network security in smart cities

Between 2013 and 2019, research on network security is a critical aspect of smart cities, requiring robust measures to maintain integrity and confidentiality. Embedded systems, big data, automation, and wireless sensors are essential components in creating an integrated ecosystem for various services. Effective data management, analysis, and protection are crucial for the operational sustainability and security of smart city systems. Automation is also vital for efficient operations. However, identifying and addressing potential vulnerabilities is essential for maintaining network security (Mohammadi et al., 2019). Wireless sensors in smart city infrastructure pose security risks, and protecting

data sent and received by these sensors is another challenge. A comprehensive conceptual framework for smart city security involves understanding potential threats, formulating appropriate security policies, and implementing necessary technologies to protect networks (Parasol, 2018). This framework helps coordinate efforts in managing data security and automation systems, ensuring the sustainability and success of smart cities.

A conceptual framework is essential for guiding the design and implementation of effective security strategies in smart city networks. This framework should consider the complexity of the ecosystem, involve stakeholders, and incorporate the latest technologies to maintain holistic network security. (Wirtz et al., 2019) Thus, network security research in smart cities in 2019 not only covers technical aspects but also emphasizes the importance of developing a robust conceptual framework to maintain data integrity and confidentiality in this increasingly connected environment.

In 2020, research on network security in smart cities focused on the interconnectedness of IoT, intelligent buildings, smart cities, and sensors (Bibri, 2020). IoT enables physical objects to connect and exchange data over the internet, which is crucial in optimizing city functionality. Smart buildings, which use technology to enhance operational efficiency, safety, and comfort, are also interconnected and a focal point in network security. As smart cities grow, network sustainability and security within smart buildings become increasingly essential aspects that must be studied and optimized.

Smart cities rely heavily on sensors for collecting data like weather, air quality, and traffic, which is crucial for decision-making and resource management. However, security vulnerabilities in these sensors can expose them to potential threats (O. Ali et al., 2020). In 2020, research focused on integrating IoT technologies securely, ensuring network security in smart buildings, managing sensor data, and identifying potential security risks in smart city environments. Understanding the relationship between IoT, intelligent buildings, smart cities, and sensors is essential for developing effective and adaptive network security solutions in the smart city era.

The 2021 research highlights the intricate interplay between network security, the internet, sustainability, datasets, and AI in smart cities (Adi Bhaskara & Nurmandi, 2022). Network security challenges have grown with increasing internet connectivity, necessitating a comprehensive approach. Sustainability is crucial as smart cities seek eco-friendly, efficient resource use. With growing data sets, data analysis is essential for detecting security threats and optimizing operations, but protecting data integrity and privacy requires robust security technologies.

AI is crucial in improving network security in smart cities, detecting abnormal patterns, and responding to attacks. However, ethical and security concerns arise from its use in security decision-making (Braga et al., 2021). Key trends include AI algorithms for managing large datasets while considering sustainability. Addressing security risks and implementing sustainable solutions are essential for building safe, efficient, and sustainable smart cities.

The 2022 research on network security in smart cities focuses on key interrelated factors such as information management, COVID-19, quality of life, artificial neural networks, and deep learning (Javed et al., 2022). Information management is essential to maintain critical data availability, integrity, and confidentiality for smart city operations. The COVID-19 pandemic has increased the risk of cyberattacks due to increased reliance on digital infrastructure.

The results of this research emphasize various essential solutions to investigate creative security tactics to keep smart city infrastructure and services safe amidst the global crisis. Quality of life is also an important consideration, as excellent network security can improve the quality of life of smart city residents. Artificial neural networks

and deep learning can help identify complex attack patterns and improve the adaptation of security systems to new threats. Understanding these complex relationships will help develop effective and adaptable security systems in the future.

The main contribution of this research to theory is in solving the increasing security problems in smart city environments. This idea paves the way for creating more responsive and complex security systems by focusing on artificial intelligence and deep learning. Artificial neural networks are used to identify complex attack patterns, while deep learning increases the system's capacity to learn and adapt to new emerging threats.

The study highlights the importance of adaptive security systems in smart city environments, combining artificial intelligence and deep learning. These systems detect complex attack patterns and quickly adapt to new threats, thereby enhancing the security of infrastructure and services, ultimately improving the lives of smart city citizens.

The Topic of IoT in smart cities

Figure 6 shows relationship keywords for the IoT in smart cities with co-occurrence overlay visualization. The color intensity of the overlay network indicates the number of publications, with deeper colors representing older publications and brighter yellowish colors depicting more recent research. This visualization helps identify significant trends, critical moments in research history, and areas that need more attention.

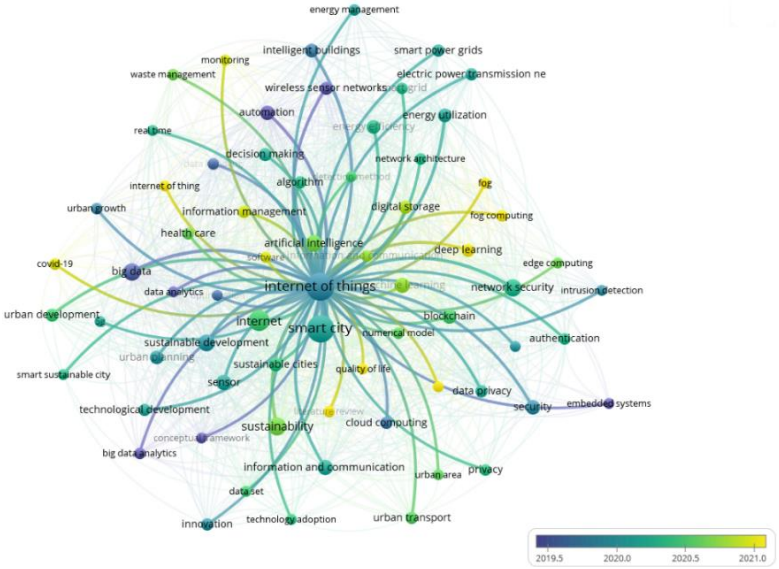

Figure 6. Relationship keyword of IoT in smart cities

Between 2013 and 2019, IoT became a significant research focus, particularly in developing smart cities. Data analytics plays a crucial role in processing and analyzing information collected by connected devices in an IoT environment, providing valuable insights for decision-making (Borgogno & Colangelo, 2019; Hsu & Lin, 2016; Wirtz et al., 2019). IoT integrates various systems in intelligent buildings, such as energy management, security, and occupant comfort, improving operational efficiency and optimizing resource usage (Araszkiewicz, 2017; Konstantakopoulos et al., 2019).

Security is a crucial aspect of IoT implementation, with efforts being made to develop intelligent intrusion detection systems. The smart city concept is also a significant focus, as the widespread adoption of IoT technologies can increase the risk of cyberattacks and other security threats (Kimani et al., 2019; Parasol, 2018). Integrating IoT with a smart sustainable city offers opportunities to optimize resource use sustainably. Data analytics plays a crucial role in understanding and managing the environmental impact of IoT implementation in a smart sustainable city.

In 2020, IoT research in smart cities focused on integrating blockchain, energy efficiency, AI, and detection methods. Blockchain is a secure and decentralized data distribution technology that enhances security and transparency in the IoT ecosystem (Dutta et al., 2020). It ensures data integrity, device authentication, and transaction security, forming a solid foundation for a secure IoT ecosystem. Energy efficiency is a critical focus in creating sustainable smart cities, enabling real-time monitoring and management of energy consumption.

AI plays a crucial role in analyzing data generated by IoT sensors, providing insights, and supporting smart decision-making (Kashef et al., 2021). Detection methods, an integral part of IoT infrastructure, offer a systematic approach to identifying security threats, device failures, and operational issues. These technologies improve emergency response, ensure system reliability, and enhance public safety. The research aims to address the complex challenges of managing city growth and improving the quality of life for residents.

In 2021, IoT became the primary focus of research in smart cities. The relationship between machine learning, information and communication, digital storage, and information management is crucial for understanding IoT dynamics in urban environments (Braga et al., 2021). Machine learning algorithms can analyze data collected by IoT devices, improving operational efficiency and predictive capabilities. Information and communication are essential for connectivity in the IoT ecosystem, facilitating the exchange of critical information. Efficient and secure communication protocols are required to support complex IoT operations in dense urban environments.

Digital storage is crucial for handling the extensive data generated by IoT devices, covering a wide range of information from environmental conditions to user behavior. Effective data organization and management ensure informed decision-making, and an integrated information management system simplifies data processing and analysis (Farhan HR & Nurmandi, 2022). In 2021, the comparison and integration between machine learning, information and communication, digital storage, and information management are in the spotlight. Researchers are exploring synergistic interactions between these technologies to improve efficiency, security, and sustainability in the implementation of IoT in smart cities.

In 2022, research on IoT in smart cities focused on the relationship between monitoring, software, information management, COVID-19, quality of life, artificial neural networks, deep learning, and fog computing (Goel & Vishnoi, 2022). Monitoring is crucial for understanding environmental dynamics, such as air pollution, temperature, and population density. Software is vital in analyzing sensor-generated data, enabling real-time interpretation and quick decision-making.

Information management is essential for improving infrastructure efficiency, providing better services to citizens, and managing city resources. COVID-19-related research is emerging (Kawuriyan et al., 2022), with IoT used for public health monitoring, contact tracing, and disease spread management. Integrating data from health sensors with IoT technology and analysis using artificial neural networks and deep learning enables pattern identification for pandemic management and control.

Quality of life in smart cities is a key focus, with IoT technology improving convenience, safety, and efficient resource use. Fog computing, where data processing is distributed and closest to the data source, reduces latency and improves system responsiveness. The trend research highlights the interconnectedness of monitoring, software, information management, COVID-19, quality of life, artificial neural networks, deep learning, and fog computing in developing effective IoT solutions for smart cities.

Research on IoT technology and fog computing in smart cities has shown great potential in improving quality of life. Fog computing reduces latency and improves system responsiveness, enhancing security, resource-use efficiency, and convenience for city residents. The interconnection between monitoring, information management, and technologies like artificial neural networks and deep learning is crucial for developing IoT solutions for smart cities. By collecting and processing data carefully, cities can design adaptive solutions.

Research on COVID-19 and IoT technologies emphasizes the importance of innovative solutions to global health challenges. These technologies have helped develop health monitoring systems, track virus spread, and regulate health resource availability. However, challenges such as data privacy and robust infrastructure are needed to ensure the sustainability and security of these technologies.

CONCLUSION

Research and publications on network and IoT security issues in smart cities have increased in the last ten years. This study emphasizes the importance of network security and IoT in smart cities, which aim to improve operational efficiency, convenience, and quality of life. IoT technologies collect and exchange data, providing benefits like traffic monitoring and waste management. However, they also present complex security challenges as the number of connected devices increases. Smart cities focus on sustainability, utilizing technology to improve environmental quality, manage resources efficiently, and address social issues. Network security is critical for maintaining data integrity in complex networks, while big data is essential for managing IoT data. AI and machine learning can detect security threats and improve network response to dynamic changes.

Network security in smart cities is crucial for maintaining data integrity and confidentiality. It involves integrating embedded systems, big data, automation, and wireless sensors for operational sustainability. Effective data management and protection are essential for this. Research on the complex interactions between network security, internet, sustainability, data sets, and artificial intelligence is essential for designing adaptive strategies. Understanding these elements is key to creating effective and adaptable network security solutions in the increasingly complex smart city environment.

Integrating IoT technologies in smart cities is gaining significant attention, with data analytics playing an essential role in decision-making. Blockchain, energy efficiency, AI, and detection methods are being integrated to improve security and transparency. Machine learning algorithms are also being explored for operational efficiency and predictive capabilities. Recent studies have shifted the focus to monitoring, software, information management, COVID-19, quality of life, artificial neural networks, deep learning, and fog computing. These interconnected aspects are critical to developing effective IoT solutions in smart cities, improving convenience, security, and resource efficiency.

Further research is needed to improve network security and IoT implementation in smart cities. This includes developing advanced security techniques, integrating big data and sustainability, focusing on data security, and exploring blockchain integration. In addition, research should also explore the application of innovative technologies such as blockchain in network security and develop solutions to monitor and manage crises. These efforts can improve efficiency, convenience, and quality of life in an increasingly connected urban society.

REFERENCE

Adi Bhaskara, J., & Nurmandi, A. (2022). Role of Artificial Intelligence in the Smart City: A Bibliometric Review. In *Communications in Computer and Information Science: Vol. 1655 CCIS* (pp. 589–596). Springer. https://doi.org/10.1007/978-3-031-19682-9_74

Afaq, A., Haider, N., Baig, M. Z., Khan, K. S., Imran, M., & Razzak, I. (2021). Machine learning for 5G security: Architecture, recent advances, and challenges. *Ad Hoc Networks*, *123*, 102667. https://doi.org/10.1016/j.adhoc.2021.102667

Ahanger, T. A., Aljumah, A., & Atiquzzaman, M. (2022). State-of-the-art survey of artificial intelligent techniques for IoT security. *Computer Networks*, *206*, 108771. https://doi.org/10.1016/j.comnet.2022.108771

Ali, O., Shrestha, A., Chatfield, A., & Murray, P. (2020). Assessing information security risks in the cloud: A case study of Australian local government authorities. *Government Information Quarterly*, *37*(1), 101419. https://doi.org/10.1016/j.giq.2019.101419

Ali, S. E. A., Lai, F. W., Dominic, P. D. D., Brown, N. J., Lowry, P. B. B., & Ali, R. F. (2021). Stock market reactions to favorable and unfavorable information security events: A systematic literature review. *Computers and Security*, *110*, 102451. https://doi.org/10.1016/j.cose.2021.102451

Araszkiewicz, K. (2017). Digital Technologies in Facility Management - The state of Practice and Research Challenges. *Procedia Engineering*, *196*, 1034–1042. https://doi.org/10.1016/j.proeng.2017.08.059

Ashraf, J., Keshk, M., Moustafa, N., Abdel-Basset, M., Khurshid, H., Bakhshi, A. D., & Mostafa, R. R. (2021). IoTBoT-IDS: A novel statistical learning-enabled botnet detection framework for protecting networks of smart cities. *Sustainable Cities and Society*, *72*. https://doi.org/10.1016/j.scs.2021.103041

Atitallah, S. Ben, Driss, M., & Ghzela, H. Ben. (2022). Microservices for Data Analytics in IoT Applications: Current Solutions, Open Challenges, and Future Research Directions. *Procedia Computer Science*, *207*, 3938–3947. https://doi.org/10.1016/j.procs.2022.09.456

Axelsson, K., & Granath, M. (2018). Stakeholders' stake and relation to smartness in smart city development: Insights from a Swedish city planning project. *Government Information Quarterly*, *35*(4), 693–702. https://doi.org/10.1016/j.giq.2018.09.001

Bader, L., Pennekamp, J., Matzutt, R., Hedderich, D., Kowalski, M., Lücken, V., & Wehrle, K. (2021). Blockchain-based privacy preservation for supply chains supporting lightweight multi-hop information accountability. *Information Processing and Management*, *58*(3), 102529. https://doi.org/10.1016/j.ipm.2021.102529

Barbosa, M. W. (2021). Uncovering research streams on agri-food supply chain management: A bibliometric study. *Global Food Security*, *28*, 100517. https://doi.org/10.1016/j.gfs.2021.100517

Benyahya, M., Collen, A., Kechagia, S., & Nijdam, N. A. (2022). Automated city shuttles: Mapping the key challenges in cybersecurity, privacy and standards to future developments. *Computers and Security*, *122*. https://doi.org/10.1016/j.cose.2022.102904

Bibri, S. E. (2020). Compact urbanism and the synergic potential of its integration with data-driven smart urbanism : An extensive interdisciplinary literature review. *Land Use Policy*, *97*. https://doi.org/10.1016/j.landusepol.2020.104703

Borgogno, O., & Colangelo, G. (2019). Data sharing and interoperability: Fostering innovation and competition through APIs. *Computer Law and Security Review*, *35*(5), 105314. https://doi.org/10.1016/j.clsr.2019.03.008

Braga, I. F. B., Ferreira, F. A. F., Ferreira, J. J. M., Correia, R. J. C., Pereira, L. F., & Falcão, P. F. (2021). A DEMATEL analysis of smart city determinants. *Technology in Society*, *66*, 101687. https://doi.org/10.1016/j.techsoc.2021.101687

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

Chen, C. (2017). Science Mapping: A Systematic Review of the Literature. *Journal of Data and Information Science*, *2*(2), 1–40. https://doi.org/10.1515/jdis-2017-0006

Chen, C., & Song, M. (2019). Visualizing a field of research: A methodology of systematic scientometric reviews. *PLoS ONE*, *14*(10). https://doi.org/10.1371/journal.pone.0223994

Choudhary, S., & Meena, G. (2022). Internet of Things: Protocols, Applications and Security Issues. *Procedia Computer Science*, *215*, 274–288. https://doi.org/10.1016/j.procs.2022.12.030

Crible, L., & Degand, L. (2021). Co-occurrence and ordering of discourse markers in sequences: A multifactorial study in spoken French. *Journal of Pragmatics*, *177*, 18–28. https://doi.org/10.1016/j.pragma.2021.02.006

Davis, P. A. E. (2022). Decrypting Australia's 'Anti-Encryption' legislation: The meaning and effect of the 'systemic weakness' limitation. *Computer Law and Security Review*, *44*, 105659. https://doi.org/10.1016/j.clsr.2022.105659

Djen, R. A. M., Nurmandi, A., Muallidin, I., Kurniawan, D., & Loilatu, M. J. (2023). Artificial Intelligence: Bibliometric Analysis in Government Studies. *Lecture Notes in Networks and Systems*, *465*, 411–418. https://doi.org/10.1007/978-981-19-2397-5_39

Dutta, P., Choi, T. M., Somani, S., & Butala, R. (2020). Blockchain technology in supply chain operations: Applications, challenges and research opportunities. *Transportation Research Part E: Logistics and Transportation Review*, *142*, 102067. https://doi.org/10.1016/j.tre.2020.102067

Elahi, M. M., Rahman, M. M., & Islam, M. M. (2022). An efficient authentication scheme for secured service provisioning in edge-enabled vehicular cloud networks towards sustainable smart cities. *Sustainable Cities and Society*, *76*, 103384. https://doi.org/10.1016/j.scs.2021.103384

Ennas, G., & Di Guardo, M. C. (2015). Features of top-rated gold open access journals: An analysis of the scopus database. *Journal of Informetrics*, *9*(1), 79–89. https://doi.org/10.1016/j.joi.2014.11.007

Farhan HR, M., & Nurmandi, A. (2022). Government Data Processing Mechanism to Support Smart City: A Bibliometric Review. In *Communications in Computer and Information Science: Vol. 1655 CCIS* (pp. 498–506). Springer. https://doi.org/10.1007/978-3-031-19682-9_63

Farooq, U., Tariq, N., Asim, M., Baker, T., & Al-Shamma'a, A. (2022). Machine learning and the Internet of Things security: Solutions and open challenges. *Journal of Parallel and Distributed Computing*, *162*, 89–104. https://doi.org/10.1016/j.jpdc.2022.01.015

Firouzi, F., Farahani, B., & Marinšek, A. (2022). The convergence and interplay of edge,

fog, and cloud in the AI-driven Internet of Things (IoT). *Information Systems*, *107*, 101840. https://doi.org/10.1016/j.is.2021.101840

Franchina, L., Inzerilli, G., Scatto, E., Calabrese, A., Lucariello, A., Brutti, G., & Roscioli, P. (2021). Passive and active training approaches for critical infrastructure protection. *International Journal of Disaster Risk Reduction*, *63*, 102461. https://doi.org/10.1016/j.ijdrr.2021.102461

Gkioulos, V., & Chowdhury, N. (2021). Cyber security training for critical infrastructure protection: A literature review. *Computer Science Review*, *40*, 100361. https://doi.org/10.1016/j.cosrev.2021.100361

Goel, R. K., & Vishnoi, S. (2022). Urbanization and sustainable development for inclusiveness using ICTs. *Telecommunications Policy*, *46*(6), 102311. https://doi.org/10.1016/j.telpol.2022.102311

Goerlandt, F., Li, J., & Reniers, G. (2022). The landscape of safety management systems research: A scientometric analysis. *Journal of Safety Science and Resilience*, *3*(3), 189–208. https://doi.org/10.1016/j.jnlssr.2022.02.003

Gyamfi, B. A., Agozie, D. Q., & Bekun, F. V. (2022). Can technological innovation, foreign direct investment and natural resources ease some burden for the BRICS economies within current industrial era? *Technology in Society*, *70*, 102037. https://doi.org/10.1016/j.techsoc.2022.102037

Hoffman, F. (2021). National Security in the Post-Pandemic Era. *Orbis*, *65*(1), 17–45. https://doi.org/10.1016/j.orbis.2020.11.002

Hsu, C. L., & Lin, J. C. C. (2016). An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives. *Computers in Human Behavior*, *62*, 516–527. https://doi.org/10.1016/j.chb.2016.04.023

Huo, C., Ma, S., & Liu, X. (2022). Hotness prediction of scientific topics based on a bibliographic knowledge graph. *Information Processing and Management*, *59*(4), 102980. https://doi.org/10.1016/j.ipm.2022.102980

Imghoure, A., El-Yahyaoui, A., & Omary, F. (2022). ECDSA-based certificateless conditional privacy-preserving authentication scheme in Vehicular Ad Hoc Network. *Vehicular Communications*, *37*, 100504. https://doi.org/10.1016/j.vehcom.2022.100504

Javed, A. R., Shahzad, F., Rehman, S. ur, Zikria, Y. Bin, Razzak, I., Jalil, Z., & Xu, G. (2022). Future smart cities requirements, emerging technologies, applications, challenges, and future aspects. *Cities*, *129*. https://doi.org/10.1016/j.cities.2022.103794

Kashef, M., Visvizi, A., & Troisi, O. (2021). Smart city as a smart service system: Human-computer interaction and smart city surveillance systems. *Computers in Human Behavior*, *124*, 106923. https://doi.org/10.1016/j.chb.2021.106923

Kawuriyan, M. W., Sadayi, D. P., Purnomo, E. P., & Fathani, A. T. (2022). Comparison of Smart Governance in Response to Handling COVID-19 (Case Study: South Tangerang City, Yogyakarta City, Surabaya City). *Webology*, *19*(1), 2768–2781. https://doi.org/10.14704/web/v19i1/web19184

Khan, Z., Pervez, Z., & Abbasi, A. G. (2017). Towards a secure service provisioning framework in a Smart city environment. *Future Generation Computer Systems*, *77*, 112–135. https://doi.org/10.1016/j.future.2017.06.031

Kimani, K., Oduol, V., & Langat, K. (2019). Cyber security challenges for IoT-based smart grid networks. *International Journal of Critical Infrastructure Protection*, *25*, 36–49. https://doi.org/10.1016/j.ijcip.2019.01.001

Konstantakopoulos, I. C., Barkan, A. R., He, S., Veeravalli, T., Liu, H., & Spanos, C. (2019). A deep learning and gamification approach to improving human-building interaction and energy efficiency in smart infrastructure. *Applied Energy*, *237*, 810–821. https://doi.org/10.1016/j.apenergy.2018.12.065

Lawelai, H., Iswanto, I., & Raharja, N. M. (2023). Use of Artificial Intelligence in Public Services: A Bibliometric Analysis and Visualization. *TEM Journal*, *12*(2), 798–807. https://doi.org/10.18421/TEM122-24

Lee-Geiller, S., & Lee, T. (David). (2019). Using government websites to enhance democratic E-governance: A conceptual model for evaluation. *Government Information Quarterly*, *36*(2), 208–225. https://doi.org/10.1016/j.giq.2019.01.003

Li, L., Taeihagh, A., & Tan, S. Y. (2022). What factors drive policy transfer in smart city development? Insights from a Delphi study. *Sustainable Cities and Society*, *84*. https://doi.org/10.1016/j.scs.2022.104008

Liu, Y. li, Huang, L., Yan, W., Wang, X., & Zhang, R. (2022). Privacy in AI and the IoT: The privacy concerns of smart speaker users and the Personal Information Protection Law in China. *Telecommunications Policy*, *46*(7), 102334. https://doi.org/10.1016/j.telpol.2022.102334

Mantelero, A., & Esposito, M. S. (2021). An evidence-based methodology for human rights impact assessment (HRIA) in the development of AI data-intensive systems. *Computer Law and Security Review*, *41*, 105561. https://doi.org/10.1016/j.clsr.2021.105561

Martín-Martín, A., Orduna-Malea, E., Thelwall, M., & Delgado López-Cózar, E. (2018). Google Scholar, Web of Science, and Scopus: A systematic comparison of citations in 252 subject categories. *Journal of Informetrics*, *12*(4), 1160–1177. https://doi.org/10.1016/j.joi.2018.09.002

Mohammadi, S., Mirvaziri, H., Ghazizadeh-Ahsaee, M., & Karimipour, H. (2019). Cyber intrusion detection by combined feature selection algorithm. *Journal of Information Security and Applications*, *44*, 80–88. https://doi.org/10.1016/j.jisa.2018.11.007

Montoya, F. G., Alcayde, A., Baños, R., & Manzano-Agugliaro, F. (2018). A fast method for identifying worldwide scientific collaborations using the Scopus database. *Telematics and Informatics*, *35*(1), 168–185. https://doi.org/10.1016/j.tele.2017.10.010

Nurmandi, A., Kurniawan, D., Misran, & Salahudin. (2021). A Meta-analysis of Big Data Security: How the Government Formulates a Model of Public Information and Security Assurance into Big Data. In *Communications in Computer and Information Science: Vol. 1499 CCIS* (pp. 472–479). Springer. https://doi.org/10.1007/978-3-030-90179-0_60

Okitasari, M., & Katramiz, T. (2022). The national development plans after the SDGs: Steering implications of the global goals towards national development planning. *Earth System Governance*, *12*, 100136. https://doi.org/10.1016/j.esg.2022.100136

Parasol, M. (2018). The impact of China's 2016 Cyber Security Law on foreign technology firms, and on China's big data and Smart City dreams. *Computer Law and Security Review*, *34*(1), 67–98. https://doi.org/10.1016/j.clsr.2017.05.022

Peron, A. E. dos R., Edler Duarte, D., Simões-Gomes, L., & Batista Nery, M. (2021). Viral surveillance: Governing social isolation in São Paulo, Brazil, during the COVID-19 Pandemic. *Social Sciences and Humanities Open*, *3*(1), 100128.

https://doi.org/10.1016/j.ssaho.2021.100128

Riahi Sfar, A., Natalizio, E., Challal, Y., & Chtourou, Z. (2018). A roadmap for security challenges in the Internet of Things. *Digital Communications and Networks*, *4*(2), 118–137. https://doi.org/10.1016/j.dcan.2017.04.003

Sánchez-Gil, S., Gorraiz, J., & Melero-Fuentes, D. (2018). Reference density trends in the major disciplines. *Journal of Informetrics*, *12*(1), 42–58. https://doi.org/10.1016/j.joi.2017.11.003

Sandeepa, C., Siniarski, B., Kourtellis, N., Wang, S., & Liyanage, M. (2022). A survey on privacy for B5G/6G: New privacy challenges, and research directions. *Journal of Industrial Information Integration*, *30*, 100405. https://doi.org/10.1016/j.jii.2022.100405

Seyhan, K., & Akleylek, S. (2022). Classification of random number generator applications in IoT: A comprehensive taxonomy. *Journal of Information Security and Applications*, *71*, 103365. https://doi.org/10.1016/j.jisa.2022.103365

Stapleton, J., Carter, C., & Bredahl, L. (2020). Developing systematic search methods for the library literature: Methods and analysis. *Journal of Academic Librarianship*, *46*(5), 102190. https://doi.org/10.1016/j.acalib.2020.102190

Syahputra, D. I., Nurmandi, A., & Subekti, D. (2023). Bibliometric Analysis of Research Publication Trends on the ICT Use in Government Institutions from 2015–2022. *Lecture Notes in Networks and Systems*, *624 LNNS*, 54–67. https://doi.org/10.1007/978-3-031-25344-7_6

Wirtz, B. W., Weyerer, J. C., & Kehl, I. (2022). Governance of artificial intelligence: A risk and guideline-based integrative framework. *Government Information Quarterly*, *39*(4), 101685. https://doi.org/10.1016/j.giq.2022.101685

Wirtz, B. W., Weyerer, J. C., & Schichtel, F. T. (2019). An integrative public IoT framework for smart government. *Government Information Quarterly*, *36*(2), 333–345. https://doi.org/10.1016/j.giq.2018.07.001

Zhang, D., Pee, L. G., Pan, S. L., & Cui, L. (2022). Big data analytics, resource orchestration, and digital sustainability: A case study of smart city development. *Government Information Quarterly*, *39*(1), 101626. https://doi.org/10.1016/j.giq.2021.101626

Zhang, D., Pee, L. G., Pan, S. L., & Liu, W. (2022). Orchestrating artificial intelligence for urban sustainability. *Government Information Quarterly*, *39*(4), 101720. https://doi.org/10.1016/j.giq.2022.101720

Zimand-Sheiner, D., & Lahav, T. (2022). Plain old Bess in a different dress? Disruptions of public relations in the digital age. *Public Relations Review*, *48*(5), 102250. https://doi.org/10.1016/j.pubrev.2022.102250