For citation purposes
Reddy, H., **Razzaque, A.**, & Mangalaraj, G. (2024). Smart cities amidst a cybersecurity dilemma: A Co-occurrence Approach. *60th MBAA International Conference.* Chicago, IL.

Smart cities amidst a cybersecurity dilemma: A Co-occurrence Approach

Hima Reddy[1]
Anjum Razzaque[2]
George Mangalaraj[3]
[1,2,3] School of Computer Sciences, College of Business and Technology,
Western Illinois University, Macomb, Illinois, USA
Emails: b-reddy@wiu.ed[1], g-mangalaraj@wiu.edu[2], a-razzaque@wiu.edu[3]

ABSTRACT
The concept of smart cities has evolved over two decades, and they rely on information communication technologies (ICT) to a great extent. ICTs are used in various ways, such as smart homes, smart transportation, smart grid, and smart health, among other things, to carry out daily activities. The use of ICTs also opens up the challenge of cybersecurity. Hence, it is important to understand the cybersecurity-related research in this area. With that in mind, this study examines the published research using bibliometric analysis to unravel the major research themes. This study identifies six dominant research themes in this area. The findings of this research will be useful to research and practice in many ways.
Keywords: Smart cities; Cybersecurity

Paper type: Literature Review paper

1. INTRODUCTION

Cities have emerged as a cornerstone of the modern world. According to a recent United Nations report, the world continues to urbanize, with 56% of the population living in urban areas in 2021 and 68% of the population in 2050 (UN 2022). With much of humanity living in urban areas, information communication technology (ICT) is pivotal in making cities livable and sustainable. Hence, in recent decades, smart cities have been gaining increasing prominence. Smart cities are defined in many ways, from using sensors and networks to policies and programs to enhancing the quality of life (Albino et al. 2015). Though there is no consistent definition of smart cities, one undeniable thing is ICT's critical role in smart cities. Hence, we adopt the definition of smart cities proposed by Ismagilova et al. (2019) that stresses the intelligent use of ICT within an interactive infrastructure to provide services impacting citizens' quality of life and sustainable management of natural resources (Ismagilova et al., 2019).

Smart cities use a variety of ICTs, such as smart energy meters, security devices, smart appliances for health and domestic life, and the Internet of Things (IoT) to monitor, control, and automate city infrastructure and services. Typically, a smart city consists of smart grids, building automation systems, uncrewed aerial vehicles, and smart Vehicles enabled by IoT sensors and the cloud platform (Baig et al., 2017). Using ICTs in smart cities brings many advantages to the citizens (Elmaghraby & Losavio, 2014), including positive social change through better governance and management of human capital (Kummitha & Crutzen 2017). Smart cities can also increase inequalities and promote a digital divide.

With the criticality of ICTs in smart cities, cybersecurity is deemed a critical infrastructure that underpins the smart cities. The increasing integration of advanced technologies in urban environments requires robust cybersecurity measures to safeguard smart city infrastructures due to the vulnerability of interconnected systems, data privacy concerns, and the potential for cyber-physical attacks on critical infrastructure (Mijwil et al., 2022). On a related note, cyberattacks against city governments have become increasingly prevalent in recent years. For example, in 2023, there were 95 cyberattacks targeting city governments across the United States[1]. Owing to the critical nature of the vulnerabilities of smart cities, the national cyber security agencies from five partner countries, including the United States, Canada, the United Kingdom, Australia, and New Zealand, have released the best cybersecurity practices in smart cities (CISA, 2023).

Owing to the prominence of cybersecurity, researchers have examined various aspects of it in the realm of smart cities. This study analyzes the existing research on cybersecurity in smart cities to map the field using the bibliometric technique of co-word analysis. Examining the research themes provides us with a glimpse of the critical research areas and also provides us with avenues for identifying fruitful research areas. Moreover, the study results are useful for practitioners to understand the major trends in the realm of cybersecurity and also see the connections between various areas within the smart cities.

Here is the structure of the paper. The following section reviews the existing research on cybersecurity in the area of smart cities. The subsequent section describes the research methodology. The following sections discuss the results of the study and discuss the findings. Finally, we conclude the study with future research directions.

2. LITERATURE REVIEW

In the contemporary era of the 21st century, Information Systems (IS) research has experienced significant growth alongside the digital age, giving rise to the concept of cybercities. These urban landscapes are navigating many cybersecurity crimes and threats, a prevalent theme in current literature. Amidst this landscape, integrating digital transformation elements becomes imperative for evaluating intelligent cities, urging future research to delve deeper into basic and applied realms. This research should intertwine the concepts of smart cities and cyberspace, demanding a heightened awareness of the cybersecurity impact on smart cities (Mijwi et al., 2022).

[1] https://therecord.media/west-virginia-city-hit-cyberattack

Delving into the intricate relationship between smart cities and cyberspace is essential for comprehending this technological landscape's dynamic challenges and opportunities. The fusion of such concepts propels urban development and brings to light cities' vulnerabilities in the digital realm. As scholars embark on this exploration, it becomes apparent that the intersection of smart cities and cyberspace is a multifaceted domain, requiring a comprehensive investigation that needs to pave the way for securing an intelligent urban ecosystem.

The emergence of smart cities as a transformative concept dates back to 2013, succeeding the evolution of information, digital, and sustainable cities. These smart cities leverage Information and Communication Technologies (ICT), employing algorithms and deploying Artificial Intelligence to contribute actively to the cultural and societal environment. Key characteristics encompass smart mobility, smart human level, and smart living (Arroub et al., 2016; Trindade et al., 2017). Advancements in the Internet of Things (IoT), big data analytics, and cloud computing from the foundation for intelligent urban ecosystems, addressing challenges such as traffic congestion, energy consumption, and public service delivery (Razzaque & Hamdan, 2020a, 2020b; Albastaki, 2021; Caragliu et al., 2022; Mijwi et al., 2022).

While navigating through the characteristics of smart cities, it becomes essential to comprehend the transformative impact such ecosystems bear on the various facets of urban life. The integration of ICT, its algorithms, and the deployment of Artificial Intelligence enhanced efficiency and shaped such cities' societal and cultural fabric. Such a transformed journey, i.e., driven by technology, requires a delicate balance between innovation and security. As smart cities evolve, they become both laboratories for progress and potential targets for cybersecurity threats, thus necessitating a careful examination of the strategies employed to ensure their resilience and sustainability.

However, the escalating reliance on cloud infrastructure raises concerns about data privacy, cybersecurity, and the overall resilience of smart city systems (Alaba et al., 2017). Responding to these challenges, researchers and practitioners propose strategies to mitigate cloud security risks, including encryption techniques, multi-factor authentication, and robust cybersecurity policies (Zhang et. al, 2017). Machine learning and Artificial Intelligence advancements are also leveraged to enhance anomaly detection and threat intelligence within smart city ecosystems (Vlajic, 2019).

The transition to cloud infrastructure has undoubtedly enhanced the capabilities of smart cities, but it comes with its challenges. The delicate balance between the advantages of cloud technology and the potential vulnerabilities it introduces calls for a comprehensive understanding. Encryption, multifaceted authentication, and cybersecurity policies are crucial pillars to fortify smart cities, making them resilient systems. The infusion of machine learning and Artificial Intelligence further increases the sophistication of the security apparatus, thus offering advanced capabilities in detecting anomalies and proactively addressing emerging threats.

It is crucial to note that the realization of a city where citizens experience the "*Internet of everything*" is currently nonexistent, even though many cities are moving toward smart cities (Chen et al., 2021). A noteworthy contradiction exists in the scholarly perspective. While some argue that fully realized smart cities are not yet actualized, others assert that these cities are already at a high risk of cyber-attacks, e.g., Li et al. (2019). Future research should address such a gap, reconciling between conceptualization and cybersecurity. The aim is to comprehensively understand the evolving cybersecurity landscape and develop strategies based on such a comprehension. This study's literature review and empirical analysis, employing VOSViewer, strive to achieve this goal.

Given the rising prominence of smart wearables, such as communication hijacking or mobile ransomware, individual users' data and personal identity within smart cities are under threat. These cybersecurity risks pose significant challenges, especially in the burgeoning development of autonomous vehicles, which operate without direct human intervention, relying on various technologies and sensors to navigate and make driving decisions (Chen et al., 2021).

Furthermore, recent years have seen extensive scholarly discussions on deep learning, a subset of machine learning (Chen et al., 2021). It has evolved from machine learning and, in turn, from Artificial Intelligence, showcasing substantial advancements in analytical learning capabilities compared to traditional machine-learning-based solutions. As smart cities evolve, navigating the complex cybersecurity landscape becomes paramount for sustainable and secure development.

3. RESEARCH METHODOLOGY

Past research on smart cities with cybersecurity has taken various approaches. For example, Ismagilova et al. (2019) reviewed journal publications focusing on security, privacy, and risks, revealing a substantial increase in studies from 2010 to 2019. Major research areas included privacy and security of mobile devices, smart city infrastructure, smart power systems, smart healthcare, frameworks and models, operational vulnerabilities, use/adoption of smart services, use of blockchain, and social media in smart cities. Laufs et al. (2020) focused on the technical aspects of cybersecurity in smart cities. They outlined interventions involving new sensors, traditional actuators, efforts to make old systems smart, and the introduction of new functionalities. Apart from reviewing research articles, researchers have also examined the technical standards and regulatory framework for cybersecurity (Vitunskaite et al. 2019), owing to the multiple stakeholders in the management of smart cities.

This study takes a different approach to surveying the research on smart cities and cybersecurity by employing the bibliometric technique of co-word analysis. In the past, such a technique get utilized to examine research on smart cities in general (Sharifi, 2021) or specific areas of smart cities, such as IoT use (Szum, 2021). However, the corpus of research in the cybersecurity area in smart cities is not subject to the large-scale use of bibliometric techniques. Hence, this study contributes to the existing discourse by providing deeper insights into the published research.

Co-occurrence Approach in Research:

To comprehend the interplay between smart cities and cloud security, scholars have adopted the co-occurrence approach, which involves analyzing the simultaneous appearance of terms in academic literature. This method enables researchers to identify patterns, trends, and key themes within the smart city-cloud security dilemma (Tang, 2018).

The co-occurrence approach is valuable for understanding the intricate relationship between smart cities and cybersecurity. As smart cities evolve, addressing the inherent security challenges associated with technologies is imperative. The literature reviewed highlights the ongoing efforts to develop resilient and secure smart city infrastructures through innovative approaches and interdisciplinary collaboration.

This study employed a systematic process to analyze research amidst smart cities and the cybersecurity realm, i.e., focusing typically on those discussed studies and investigations that intersect technology, urban development, and cybersecurity. Smart cities leverage advanced digital technologies and data analytics to enhance efficiency, sustainability, and the overall quality of residential life.

Research methodology-wise, this study is broken down into multiple phases to unravel the key themes. In this section, this study provides a comprehensive overview of how we collected and analyzed data for this research, aimed to utilize VOSviewer and apply a co-occurrence approach to identify and characterize key themes within a specific dataset, facilitating a comprehensive understanding of the underlying patterns and relationships in the data.

Data Collection

In this study's initial phase, published research data was meticulously gathered from a custom selection within ISI's Web of Science (WOS), specifically the Web of Science Core Collection. This comprehensive selection encompassed various parameters such as authors, title, source, times cited count, abstract, addresses, document type, keywords, research area, cite reference count, usage count, hot paper designation, highly cited status, as well as funding information, and publisher details, providing a thorough foundation for analysis. For further analysis, this study identified 702 research studies, including journal articles and conference proceedings.

Co-word Analysis

Co-word analysis is a technique in text mining and bibliometrics involving analysis of words' co-occurrence within a set of documents to explore relations between words that tend to appear together within similar contexts. Co-word analysis aims to identify patterns and associations between terms to reveal the thematic structure and connections within a body of text. In scientific research, social sciences, and information retrival, a technique often applies to unveil textual data's underlying structures and relationships (Singh et al., 2023).

This study aims to uncover research themes related to smart cities and cybersecurity. In pursuit of this goal, the authors conducted a co-occurrence analysis of keywords found in published research articles. The provided keywords by the authors represent the essence of their work and play a crucial role in capturing the research themes in our study.

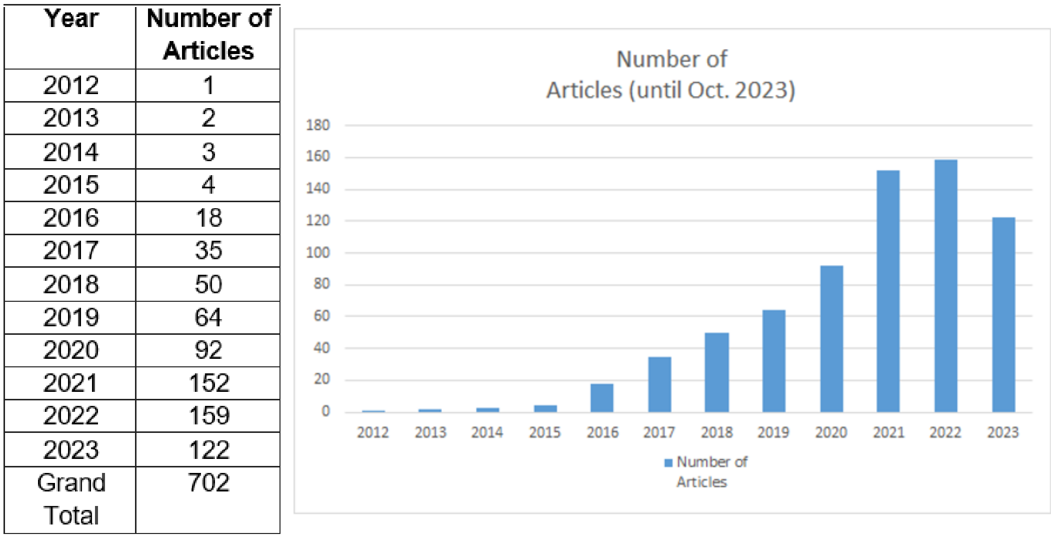
The dataset of published articles gets examined before conducting a co-word analysis, for consistency in the keyword usage. The objective was to standardize the keywords. For example, some authors have used vehicular ad hoc networks as a keyword, while others used Vanets as the keyword. Other such keywords had similar keywords, e.g., cyber-attack, cyber attack, cyber-attacks. All got replaced by cyberattacks.

Next, this study utilized VOSviewer, a tool for visualizing bibliometric networks commonly used to analyze relationships between terms, authors, or keywords in scientific publications. It creates maps illustrating connections and co-occurrences of terms, helping researchers identify patterns and key themes in literature, especially for understanding scientific field structures and recognizing influential authors (Singh et al., 2023). According to Van Eck and Waltman (2020), VOSviewer is valuable in academic research, facilitating the creation and visualization of network-based scientific maps via text mining analysis. In their conceptual explanation, they highlight using the co-occurrence analysis option, where words serve as the primary unit of analysis, resulting in an intelligent roadmap or a knowledge atlas for the research topic.

VOSviewer extracted data by generating a bibliographic map and selecting the data source as reference manager files, specifically supporting the RIS file format. The analysis involved choosing co-occurrence as the type of analysis and employing full counting as the counting method, with keywords serving as the unit of analysis. The threshold for keyword inclusion was set to a minimum count of 5 occurrences, resulting in 2973 keywords, of which 180 met the established threshold.

4. RESULTS

Figure 1 illustrates the yearly count of articles focused on cybersecurity-related smart cities articles. Notably, the initial studies on it emerged in the early 2010s, with a rapid growth in the number of publications yearly since then.



Year	Number of Articles
2012	1
2013	2
2014	3
2015	4
2016	18
2017	35
2018	50
2019	64
2020	92
2021	152
2022	159
2023	122
Grand Total	702

Figure 1. Yearly count of articles on cybersecurity in the context of smart cities

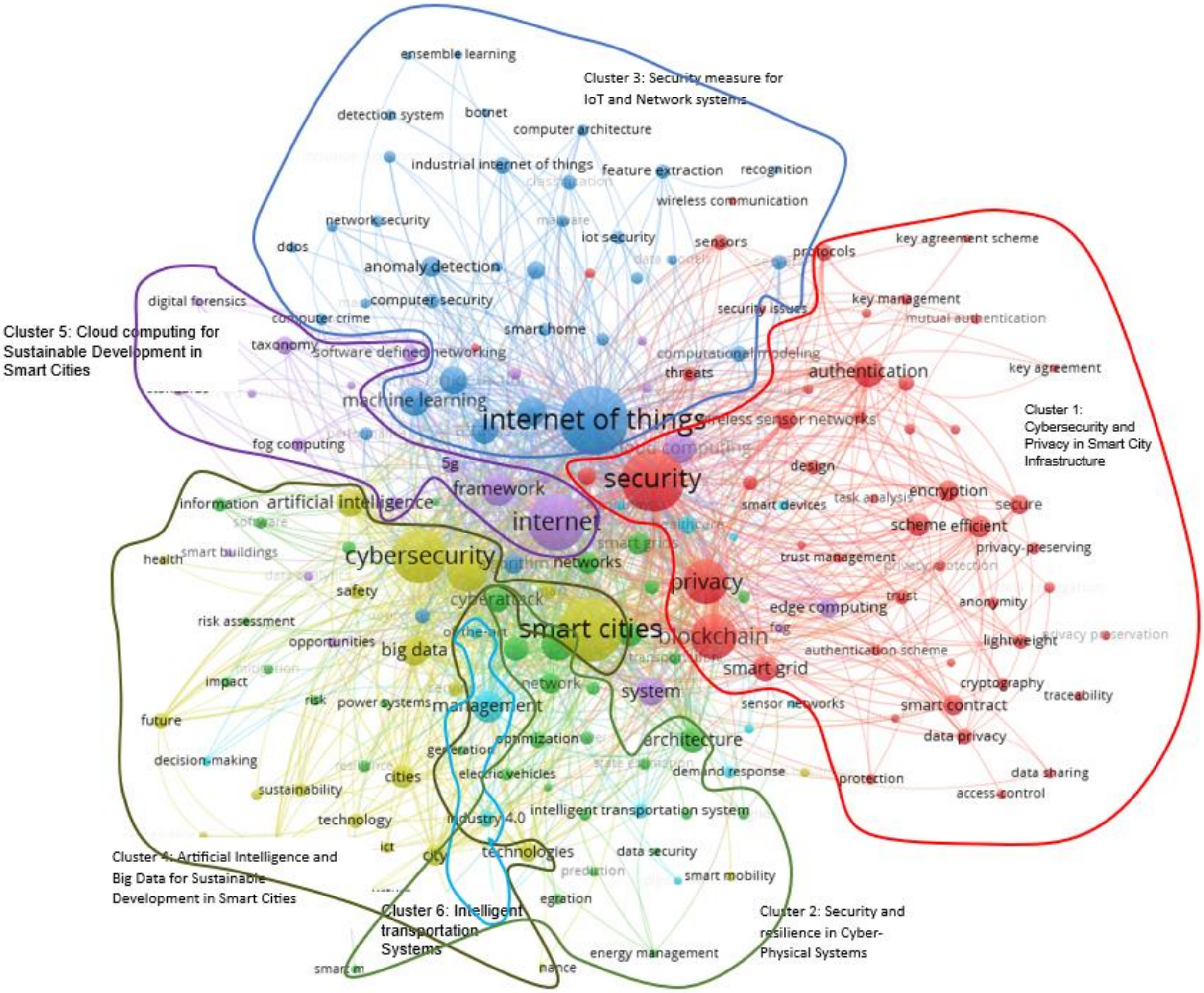
Table 1 illustrates the distribution of articles across journals, specifically focusing on those with a count greater than 5. The table highlights numerous publication outlets for research related to keywords in smart cities and cybersecurity. The diverse journal/conference avenues highlight the expansive focus areas of research streams. Moreover, it is interesting to see newer journals and conferences specifically focusing on smart cities.

Table 1: Distribution of smart cities cybersecurity research articles by outlet with count > 5

Journal/Conference Venue	**Number of articles**
IEEE Access	72
IEEE Internet of Things Journal	49
Sensors	41
Sustainable Cities and Society	34
Applied Sciences-Basel	22
Sustainability	19
Future Generation Computer Systems-The International Journal of Science	16
Computers & Security	15
Electronics	13
Energies	11
IEEE Transactions on Intelligent Transportation Systems	11
Journal of Network and Computer Applications	10
IEEE Transactions on Industrial Informatics	9
Internet of Things	9
IEEE Communications Magazine	8
IEEE Transactions on Smart Grid	8

Journal/Conference Venue	**Number of articles**
IEEE Communications Survey and Tutorials	7
Computer Communications	6
IEEE Network	6
Security and Communication Networks	6
Transactions on Emerging Telecommunications Technologies	6
Wireless Communications & Mobile Computing	6
Wireless Personal Communications	6
Buildings	5
Computer Networks	5
Concurrency and Computation-Practice & Experience	5
Microprocessors and Microsystems	5
Multimedia Tools and Applications	5
Other outlets	287
Total articles	**702**

Next, we used VOSviewer to create the cluster maps of the keywords, and Figure 3 presents the results. Moreover, VOSviewer also provided a list of clusters with related keywords, and Table 2 presents these results. Two authors reviewed the cluster composition and labeled them for further analysis.



Cluster 3: Security measure for IoT and Network systems

Cluster 5: Cloud computing for Sustainable Development in Smart Cities

Cluster 1: Cybersecurity and Privacy in Smart City Infrastructure

Cluster 4: Artificial Intelligence and Big Data for Sustainable Development in Smart Cities

Cluster 6: Intelligent transportation Systems

Cluster 2: Security and resilience in Cyber-Physical Systems

Figure 3. Themes on Smart Cities Cybersecurity Research

Table 1: Cluster themes of keywords with prominent keywords in each of the clusters

Cluster	Themes emerging from a cluster of relative keywords	Prominent Keywords
1	Cybersecurity and Privacy in Smart City Infrastructure	Access control; authentication; blockchain; cryptography; data sharing; privacy; encryption; hardware; key agreement scheme; privacy preservation; protocols; security; sensors; key management; smart grid,
2	Security and resilience in Cyber-Physical Systems	Architecture; attack detections; cyber-physical systems; data or information security; energy management; networks; software; uncertainty; vulnerability.

3	Security measures for IoT and Network systems	Algorithms; attack; botnet; computer crime; computer security; deep learning; internet of things; security; intrusion detection system; machine learning' malware; neural networks; performance; servers; smart homes.
4	Artificial Intelligence and Big Data for Sustainable Development in Smart Cities	Artificial Intelligence; big data; challenges; governance; health; ICT; infrastructure; smart mobility; sustainability; sustainable development technologies.
5	Cloud Computing for Sustainable Development in Smart Cities	5G, automation; cloud computing; edge / fog computing; real-time systems, service; smart building; software-defined networks; taxonomy; autonomous/unmanned vehicles; virtualization,
6	Intelligent Transportation Systems	Big data analytics; decision-making; Intelligence; intelligent transportation management; security challenges; sensor networks; smart devices.

5. DISCUSSION

Co-word analysis revealed various cluster themes in the cybersecurity research in the smart cities area. With the new smart cities concept and the evolving nature of cyber security concerns, it is interesting to see research in a wide-ranging area. In this section, we discuss each cluster theme and the associated research on smart cities using some exemplary research.

5.1 Cluster 1: Cybersecurity and Privacy in Smart City Infrastructure:

Smart cities collect elaborate amounts of data on various aspects through sensors and other means. Hence, it is no wonder that the security and privacy of this data are major themes in the research. Security and privacy challenges for smart cities emerge from various sources. For example, data sharing and mining with data from multiple stakeholders, data mashups, security data in the cloud, secondary use of collected data, and threats with AI are major challenges in the smart city arena (Braun et al., 2018). Khatoun & Zeadally (2017) discuss various security and privacy challenges with smart cities and present potential solutions involving organizational, technical, human, and legal aspects in overcoming them.

5.2 Cluster 2: Security and resilience in Cyber-Physical Systems (CPS):

Owing to the smart cities' dependence on ICTs and the concomitant cybersecurity challenges, issues with vulnerability and resilience have come to focus. Nova (2022) examined threat intelligence's role in providing resilience to the ICT infrastructure in smart cities. While Nova (2022) examined the role of threat intelligence, Andrade et al. (2021) took a broader view of cybersecurity issues. They examined the resilience of specific areas of smart cities, such as smart health, transportation, and others, and related to UN sustainable goals. With CPS playing a major role in smart cities, Habibzadeh et al. (2019) delve into the critical aspects of cybersecurity, data privacy, and policy challenges associated with the implementation of CPS in smart cities and highlight the increasing integration of digital technologies in smart cities and the subsequent rise in vulnerabilities, emphasizing the need for robust cybersecurity measures.

5.3 Cluster 3: Security measure for IoT and Network systems:

IoT allows various embedded devices to work together to offer services in a smart city. IoT generates vast amounts of data and can get used for safety, efficiency, infotainment applications, and services for the citizens of the smart city (Gharaibeh et al. 2017). Owing to the importance of security with these devices and sensors, Andrade et al. (2020) explore various dimensions of IoT security, aiming to provide a holistic understanding and solutions for the challenges posed by integrating IoT technologies in urban environments. The authors conduct an in-depth analysis of cybersecurity threats and vulnerabilities associated with IoT devices in smart cities, addressing issues such as data privacy, authentication, and network security.

5.4 Cluster 4: Artificial Intelligence and Big Data for Sustainable Development in Smart Cities:

Smart cities allow for generating enormous amounts of data through various systems. Apart from privacy issues that get discussed elsewhere, this data gets used by AI and machine learning tools to serve the community better. Ullah et al. (2020) review works in this area and found AI/ML's application in intelligent transportation systems, energy-efficient utilization of smart grids, effective use of uncrewed aerial vehicles (UAVs) to ensure the best services in communications, and smart health care system in a smart city. They also highlight the importance of cybersecurity and the challenges in this area.

5.4 Cluster 5: Cloud Computing for Sustainable Development in Smart Cities:

Cloud security challenges in smart cities are multifaceted. Moreover, cloud computing is extensively used in smart cities to integrate various pieces of physical infrastructure and resultant data collection methods. Hence, data breaches, unauthorized access, and service disruption pose significant threats to the integrity of smart city infrastructure (Yaqoob et al., 2017). Furthermore, cloud environments' scalability and dynamic nature exacerbate security concerns, requiring innovative solutions to safeguard sensitive information (Al-Fuqaha et al., 2015). Giannakoulias (2016) examined the issues in adopting public and various cloud service models for smart cities. They discussed the legal implications, regulatory and standards compliance, and new attack vectors resulting from vulnerabilities in the move to the cloud.

5.5 Cluster 6: Intelligent Transportation Systems:

One of the cornerstones of smart cities is the presence of intelligent transportation systems. Smart cities are redefining existing transportation management and engendering newer transportation mechanisms such as autonomous vehicles, drones, air taxis, etc. Vattapparamban et al. (2016)

explore the challenges and concerns of integrating drones in smart city environments, such as cybersecurity, privacy, and public safety. They highlight the potential risks and vulnerabilities that arise from the increased use of drones in smart cities. Mecheva and Kakanakov (2020) outline the general contours of an architecture for intelligent transportation systems and security issues that get considered.

In summary, this study revealed six prominent research themes. Examining the cluster themes, we could see the pervasiveness of cybersecurity concerns within the smart cities. The concept of smart cities evolved in the 2000s, and the rapid growth of research in this area shows the importance of cybersecurity implications in this context.

6. CONCLUSIONS AND FUTURE RESEARCH DIRECTIONS

Smart cities have become a major aspect of the modern urban development environment. ICTs play a significant role in making cities smarter, opening up many security implications. With the increased focus on cybersecurity in recent years, it is important to understand the existing research and find avenues for future research. We examine the corpus of research in cybersecurity-related areas in smart cities. Using the co-occurrence of keywords approach and bibliometric method, we arrived at six cybersecurity-related smart cities research themes.

Though the research themes identified in the study are distinct, it is important to note that they are interrelated to some extent. However, identifying the broad themes helps not only in understanding current research but also can help situate technologies and threats emerging in the future. For example, newer developments in cryptography, such as quantum key distribution, could still pertain to the first theme of security and privacy measures in smart cities. Researchers could use advanced natural language processing techniques like topic modeling to conduct a fine-grained analysis of the existing corpus of research in this area in the future.

REFERENCES

Albastaki, Yousif. "Clustering algorithms as a tool for odour classifications in enose developments." *European, Asian, Middle Eastern, North African Conference on Management & Information Systems*. Cham: Springer International Publishing, 2021.

Albino, Vito, Umberto Berardi, and Rosa Maria Dangelico. "Smart cities: Definitions, dimensions, performance, and initiatives." Journal of urban technology 22.1 (2015): 3-21.

Andrade, Roberto Omar, et al. "A comprehensive study of the IoT cybersecurity in smart cities." IEEE Access 8 (2020): 228922-228941.

Andrade, Roberto O., et al. "Cybersecurity, sustainability, and resilience capabilities of a smart city." *Smart Cities and the UN SDGs*. Elsevier, (2021). 181-193.

Arroub, Ayoub, et al. "A literature review on Smart Cities: Paradigms, opportunities and open problems." 2016 International conference on wireless networks and mobile communications (WINCOM). IEEE, 2016.

Baig, Zubair A., et al. "Future challenges for smart cities: Cyber-security and digital forensics." *Digital Investigation* 22 (2017): 3-13.

Braun, Trevor, et al. "Security and privacy challenges in smart cities." Sustainable cities and society 39 (2018): 499-507.

Caragliu, Andrea, and Chiara F. Del Bo. "Smart cities and urban inequality." *Regional Studies* 56.7 (2022): 1097-1112.

Chen, Dongliang, Paweł Wawrzynski, and Zhihan Lv. "Cyber security in smart cities: a review of deep learning-based applications and case studies." *Sustainable Cities and Society* 66 (2021): 102655.

Cui, Lei, et al. "Security and privacy in smart cities: Challenges and opportunities." IEEE Access 6 (2018): 46134-46145.

Cybersecurity Infrastructure Security Agency - CISA, "Cybersecurity Best Practices for Smart Cities", (2023), "https://www.cisa.gov/resources-tools/resources/cybersecurity-best-practices-smart-cities, April 19 2023.

Elmaghraby, Adel S., and Michael M. Losavio. "Cyber security challenges in Smart Cities: Safety, security and privacy." Journal of advanced research 5.4 (2014): 491-497.

Gharaibeh, Ammar, et al. "Smart cities: A survey on data management, security, and enabling technologies." IEEE Communications Surveys & Tutorials 19.4 (2017): 2456-2501.

Giannakoulias, Alkiviadis. "Cloud computing security: protecting cloud-based smart city applications." *Journal of Smart Cities* 2.1 (2016): 66-77.

Habibzadeh, Hadi, et al. "A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities." *Sustainable Cities and Society* 50 (2019): 101660.

Ismagilova, Elvira, et al. "Smart cities: Advances in research—An information systems perspective." International journal of information management 47 (2019): 88-100.

Khatoun, Rida, and Sherali Zeadally. "Cybersecurity and privacy solutions in smart cities." *IEEE Communications Magazine* 55.3 (2017): 51-59.

Kummitha, Rama Krishna Reddy, and Nathalie Crutzen. "How do we understand smart cities? An evolutionary perspective." Cities 67 (2017): 43-52.

Laufs, Julian, Hervé Borrion, and Ben Bradford. "Security and the smart city: A systematic review." Sustainable cities and society 55 (2020): 102023.

Li, Weiwei, et al. "Assessment of coordinated development between social economy and ecological environment: Case study of resource-based cities in Northeastern China." *Sustainable Cities and Society* 59 (2020): 102208.

Mijwil, Maad, et al. "Cybersecurity Challenges in Smart Cities: An Overview and Future Prospects." *Mesopotamian journal of cybersecurity* 2022 (2022): 1-4.

Mecheva, Teodora, and Nikolay Kakanakov. "Cybersecurity in intelligent transportation systems." *Computers* 9.4 (2020): 83

Nova, Kannan. "Security and Resilience in Sustainable Smart Cities through Cyber Threat Intelligence." *International Journal of Information and Cybersecurity* 6.1 (2022): 21-42.

Razzaque, Anjum, and Allam Hamdan. "Internet of things for learning styles and learning outcomes improve e-learning: A review of literature." *Proceedings of the International Conference on Artificial Intelligence and Computer Vision (AICV2020)*. Springer International Publishing, 2020.

Razzaque, Anjum, and Allam Hamdan. "Role of financial technology fintech: A survey." *Proceedings of the International Conference on Artificial Intelligence and Computer Vision (AICV2020)*. Springer International Publishing, 2020.

Sharifi, Ayyoob, et al. "Three decades of research on smart cities: Mapping knowledge structure and trends." Sustainability 13.13 (2021): 7140.

Singh, A., & Mangalaraj, G. "The Intellectual Structure of Social Engineering Research: A Co-occurrence Approach". DSI Annual Conference, (2023) (pp. 1-13). Atlanta.

Szum, Katarzyna. "IoT-based smart cities: A bibliometric analysis and literature review." *Engineering Management in Production and Services* 13.2 (2021): 115-136.

Trindade, Evelin Priscila, et al. "Sustainable development of smart cities: A systematic review of the literature." *Journal of Open Innovation: Technology, Market, and Complexity* 3.3 (2017): 1-14.

Ullah, Zaib, et al. "Applications of artificial intelligence and machine learning in smart cities." *Computer Communications* 154 (2020): 313-323.

UN, "World Citities Report 2022", https://unhabitat.org/wcr/

van Eck, N. J., & Waltman, L. (2020, April 1). VOSviewer Manual. Retrieved from Manual_VOSviewer_1.6.15: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.vosviewer.com/documentation/Manual_VOSviewer_1.6.15.pdf

Vattapparamban, Edwin, et al. "Drones for smart cities: Issues in cybersecurity, privacy, and public safety." *2016 international wireless communications and mobile computing conference (IWCMC)*. IEEE, 2016.

Vitunskaite, Morta, et al. "Smart cities and cyber security: Are we there yet? A comparative study on the role of standards, third party risk management and security ownership." *Computers & Security* 83 (2019): 313-331.