information

Review

Initial Cybersecurity Framework in the New Capital City of Indonesia: Factors, Objectives, and Technology

Dana Indra Sensuse [1,*], Prasetyo Adi Wibowo Putro [1], Rini Rachmawati [2] and Wikan Danar Sunindyo [3]

[1] Faculty of Computer Science, Universitas Indonesia, Depok 16424, Indonesia
[2] Department of Development Geography, Faculty of Geography, Universitas Gadjah Mada, Yogyakarta 55281, Indonesia
[3] School of Electrical Engineering and Informatics, Institut Teknologi Bandung, Bandung 40132, Indonesia
* Correspondence: dana@cs.ui.ac.id

Abstract: As a newly built city and the new capital of Indonesia, Ibu Kota Nusantara (IKN), is expected to become known worldwide as an economic driver, a symbol of national identity, and a sustainable city. As the nation's capital, IKN will become the location for running central government activities and hosting representatives of foreign countries and international organizations or institutions. However, there is no concept of cybersecurity in IKN associated with existing functions and expectations of the city. This study identifies the initial cybersecurity framework in the new capital city of Indonesia, IKN. A PRISMA systematic review was used to identify variables and design an initial framework. The initial framework was then validated by cybersecurity and smart city experts. The results show that the recommended cybersecurity framework involved IKN's factors as a livable city, a smart city, and a city with critical infrastructure. We applied five security objectives supported by risk management, governance, security awareness, and the latest security technology to these factors.

Keywords: IKN; cybersecurity; smart city; livable city; critical infrastructure; security objective; security technology; PRISMA

check for updates

Citation: Sensuse, D.I.; Putro, P.A.W.; Rachmawati, R.; Sunindyo, W.D. Initial Cybersecurity Framework in the New Capital City of Indonesia: Factors, Objectives, and Technology. *Information* **2022**, *13*, 580. https://doi.org/10.3390/info13120580

Academic Editor: Joaquim Ferreira

Received: 14 November 2022
Accepted: 9 December 2022
Published: 14 December 2022

1. Introduction

Ibu Kota Nusantara (IKN) is the official name of the new capital city of Indonesia, which will replace Jakarta. Officially, IKN will be a unique provincial-level regional government unit as its territory will be the capital city of the Republic of Indonesia [1], and and it will be managed by the IKN Authority. As the nation's capital, IKN will be the place where central government activities, representatives of foreign countries, and representatives of international organizations or institutions are located.

As a newly built city, IKN will be expected to become an economic driver, a national identity symbol, and a sustainable global city [2]. Regional development strategies, economic development, social development, human resources, land, environmental protection and management, infrastructure, displacement, and defense and security will all play a part in achieving the expectations set for IKN. Regarding security strategy, although there is no master plan for information security for IKN, there are at least three principle for the development of IKN that can be related to security, namely: realizing urban infrastructure with a circular and resilient system; creating a city that is safe, comfortable and affordable for all residents including children, women, the elderly, and persons with disabilities; creating an effective and efficient city based on technology to support governance, economic activities and the activities of its residents. With regard to these three principles, the security referred to in the IKN Master Plan is more related to having a livable city, the availability of access to critical infrastructure, and a balanced occupancy ratio.

Critical infrastructure is defined as the essential manufactured assets related to infrastructure that support the survival and well-being of a country, such as energy, water supply,

and communication [3]. Critical infrastructure is currently vulnerable to attack because of the connection to the internet as a critical information infrastructure [4]. A livable city can be defined as a comfortable place to live where various physical and non-physical activities are available [5].

Another IKN security factor related to information technology can be seen in the functions of IKN. Based on its function as the center for implementing central and local government activities, IKN is also required to implement an electronic-based government system, or SPBE [6], at the national level and the smart city concept at the world level [7]. Therefore, IKN security can also be seen as smart city security. A smart city is an urban area with modern technology that uses various types of information technology to collect specific data. The collected data is then organized to create information to manage assets, resources, and services efficiently [8]. Boyd Cohen defines six domains representing strategic areas in smart city development, which are smart government, smart living, smart economy, smart mobility, smart environment, and smart people. Therefore, the development of smart cities can be said to be the development of these domains based on innovations supported by technology. Furthermore, considering the relationship between the development of smart cities and the critical infrastructure of the government administration sector, part of security for IKN can also be defined as critical infrastructure security.

Although security is needed to ensure the achievement of expectations for IKN, there is currently a need for a cybersecurity concept that has proven compatibility with the IKN principle. Finding a practical cybersecurity concept for IKN has posed some problems since the concept is not widely discussed in scientific articles, and the phrase "new capital city" isn't a scientific keyword used in articles. Therefore, IKN cybersecurity needs to be viewed as an edge case in cybersecurity for livable cities, smart cities, and critical infrastructure.

From the current literature, there are already security discussions for each of those three fields in relation to IKN. There is a need for security in livability because many systems in use are not designed to be robust against cybercrime [9]. The cybersecurity body of knowledge defines cybersecurity as protecting information systems, their data, and the services they provide from unauthorized access, harm, or misuse. In this definition, an information system consists of hardware, software, and related infrastructure. This cybersecurity definition was created from the point of view that activities require the protection of information systems [10]. With this point of view, cybersecurity is organized with the same goals or principles as information security. The type of security control used for cybersecurity is similar to information security; however, it is used to mitigate cyber security risks in cyberspace, such as cybercrime and safety [11].

This study identifies cybersecurity concerns for Indonesia's new capital city. Identification is made through a systematic literature review related to IKN as three factors: a livable city, a smart city, and a city with critical infrastructure. A systematic literature review (SLR) is a structured and planned literature study method on the results of specific studies [12]. The aim of the SLR is not only to collect all available evidence on the research question but also to propose a framework based on the variables identified by the SLR.

This report is structured as follows. The Methodology section explains how to conduct a systematic literature review. The Results section presents the results of the data analysis, which is followed by a synthesis recommendation in the Discussion section. Finally, the report ends with a defining answer to the research question and plans for future research in the Conclusion section.

2. Methodology

This research referred to PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-analyses) [13]. PRISMA accommodates quality assessment for each literature example and assesses the strength of evidence [14]. The literature-searching strategies were developed to answer the research question, "What is the initial cybersecurity framework for IKN?" The optimized searching strategies are presented in Table 1. For the results of

the SLR, we found 17 works of literature after conducting the SLR flow diagram illustrated in Figure 1.

Table 1. Searching strategies.

Protocol Attributes	Description
Keyword	cybersecurity AND ((smart AND city) OR (livable AND city) OR (critical AND infrastructure))
Publication Type	Journal Article and Conference Proceeding
Years	2016 to 2022
Language	English
Databases	Emerald, IEEE Xplore, ProQuest, ScienceDirect, Scopus

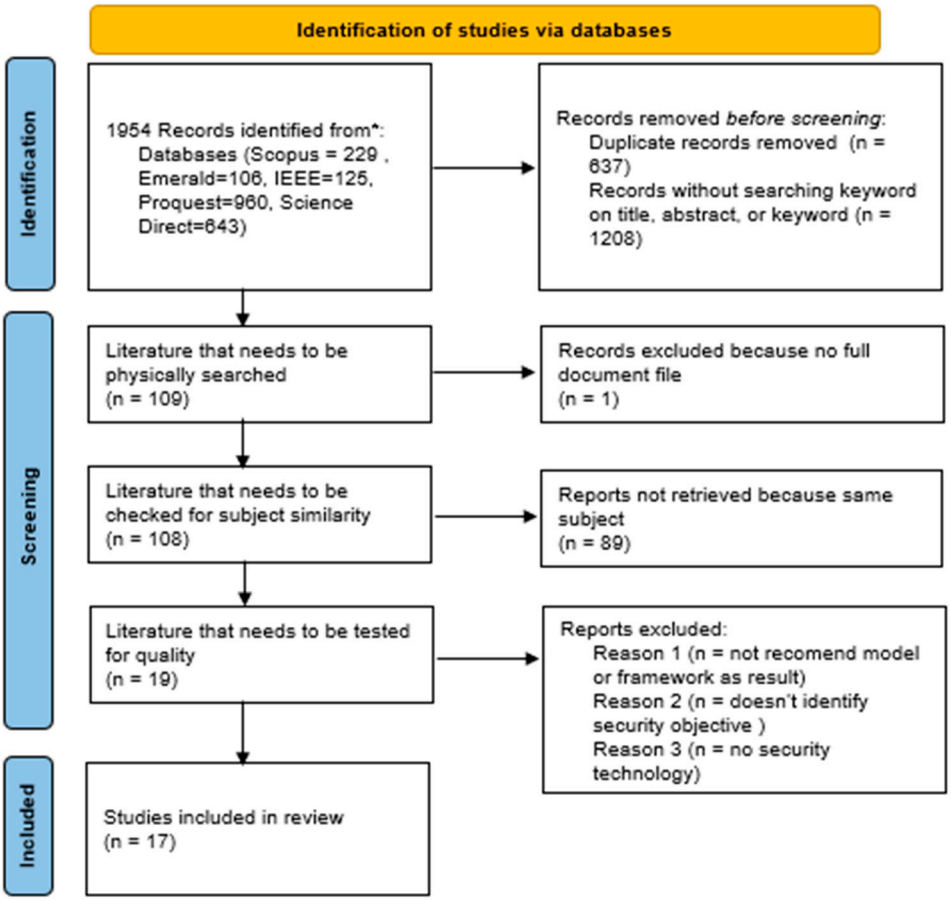

Figure 1. SLR flow diagram.

At the identification stage, a search was conducted using keywords and criteria defined in the PRISMA protocol, and 1954 articles were obtained. The results were then checked to determine whether there were similarities in the literature and whether the search keywords were available in the title, abstract, and keywords using the reference manager and spreadsheet software. For example, a similar article was found in ProQuest and Emerald [15], Scopus and IEE Xplore [16], Scopus and ProQuest [17], Scopus and Emerald [18], and Scopus and ScienceDirect [19]. After a thorough search using spreadsheet software, no search keywords were found in the abstract and keywords of several articles; thus, they had to be removed from the search results. The 5 articles above are an example of articles that were removed. Additionally, 109 articles were selected during the screening stage for the full paper to be downloaded and their quality tested.

At the screening stage, 92 articles were excluded. The screening stage removed articles for which no full paper could be obtained [20], that had no model recommendations [21],

and that had no connection to security [22]. The screening stage also eliminated articles that refined, retested, or implemented recommendations from previous articles, such as [23]. The result of the literature review included 17 pieces for analysis.

In the final step of the research, the literature review results were used to identify each variable's correlation and to design a framework. Finally, the designed framework was validated by conducting structured interviews with three experts who have worked or researched cybersecurity in the government administration sector for at least ten years.

All the SLR phases were carried out collaboratively by all authors in an iterative process considering each author's assessments. Thus, any discrepancies were discussed until a unanimous agreement was reached.

3. Results

The analysis began by looking for words related to the IKN factors and security objectives for each factor. This analysis used the word cloud feature on NVIVO 12. This study assumes that the higher the frequency is, the more scholars have the same understanding of this concept [24]. In the initial investigation, the word livability was not found in any of literature. For example, in the word cloud feature on the NVIVO 12, as seen in Figure 2, the words "infrastructure" and "smart" were found commonly with the word city, but the word "livability" was not. With further analysis using a word map, the word "infrastructure" was found in many phrases, including the word "critical". Although none of the literature used the term "livable city", two pieces of literature were associated with "livable city" using the terms "sustainable city" and "smart living".

Figure 2. Word cloud result from NVIVO 12.

Next, for the investigation into cybersecurity objectives, "privacy" and "information" were two words that often appeared in the word cloud and were mostly used with the word "security". Based on the information security objectives in ISO 27001:2022, privacy is part of the objective of information security management systems alongside information security [25]. Thus, there were four objectives found in the literature as a combination of information security and privacy protection. Those objectives were confidentiality (C), integrity (I), availability (A), and privacy (P). Other words in the word cloud, such as risk, system, and management, could not be grouped into security objectives, so they were used to identify the IKN factors or security control technologies.

The last stage of the analysis was carried out by identifying three IKN factors, the cybersecurity objectives to be achieved, and what technology is used to control security. The details of the results identified can be seen in Table 2. From 17 pieces of literature, we

found that only 1 piece of literature did not discuss smart cities, while 2 pieces of literature discussed livable cities supporting smart cities [26,27]. If associated with technological developments, livability, security, and safety were the three issues related to smart cities [26]. Safety was added into objectives because this article clearly states that a livable smart city must address security, environmental safety, and protection. In practice, livability is often mentioned together with sustainability. Livability is an issue in smart cities related to the focus of smart city development on quality of life and innovation ecosystems [27]. Aspects of critical infrastructure are also widely found in life support [26,28] and government services [28,29] in smart cities. These two critical infrastructure goals are often referred to as safety and security in the literature.

Table 2. IKN factors and security objectives.

Literature	Research Focus	IKN Factors			Objectives				
		SC	LC	CI	C	I	A	P	S
[26]	Smart City Security	x	x	x			x		x
[27]	Information Security Technology	x	x		x	x	x	x	
[28]	Natural Risk Assessment	x		x			x		
[29]	Critical Information Infrastructure Protection	x		x		x	x		
[30]	Critical Information Infrastructure Protection			x	x	x	x		
[31]	Information Security Objective	x			x	x	x	x	
[32]	Security Standard	x			x	x	x	x	
[33]	Cybersecurity Control	x			x	x	x	x	
[34]	Information Security Technology	x			x	x	x	x	
[35]	Cybersecurity Control	x			x	x	x		
[36]	Information Security Management System	x			x	x	x		
[37]	Privacy Protection	x						x	
[38]	Blockchain Authentication	x						x	
[39]	Cybersecurity Framework	x			x				
[40]	Cybersecurity Measurement	x			x		x		
[41]	Healthcare Application	x				x		x	
[42]	Smart City Security	x					x		

SC: Smart City, LC: Livable City, CI: Critical Infrastructure; C: Confidentiality, I: Integrity, A: Availability, P: Privacy, S: Safety.

Most literature recommends specific safeguards for certain threats so that only one [28,37–39,42] or two security objectives are discussed [26,29,40,41]. Although there were only 8 pieces of literature, a combination of three security objectives, namely "confidentiality", "integrity", and "availability", were also widely found [27,30–36]. In addition, some literatures combined them with privacy. Privacy was discussed if the security threat related to people's data. Another security objective identified was safety [26]. Safety was found in the literature about livable cities, especially when discussing the threat to human safety, such as a natural risk in the form of flooding.

As for technology that is used as a security control, based on the literature obtained, eleven information technologies were identified in cybersecurity, as shown in Table 3. Blockchain and Artificial Intelligence are the two most widely used information technologies. In addition, managerial technologies for risk assessment, governance, and awareness are widely recommended.

Table 3. Information technology for IKN cybersecurity.

No	Information Technology	Literature
1	Risk Assessment	[26–28]
2	Big Data	[28]
3	Governance	[29,32,35]
4	Awareness	[29–31]
5	Blockchain	[33,37,38]
6	Biometrics	[33]
7	Machine Learning	[33,37]
8	Cryptography	[33,39]
9	Network Security	[34]
10	Artificial Intelligence	[34,36,41]
11	Intrusion Detection	[40,42]

4. Discussion

Based on the literature review related to cybersecurity in IKN, the interconnection between all identified components is shown in Figure 3. Three main factors for IKN were identified as "smart city", "livable city", and "critical infrastructure". Most of the discussion was about cybersecurity in smart cities, but there is a connection between smart cities, livable cities, and critical infrastructure. A livable city is part of a smart city, focusing on innovative ecosystems and quality of life. Those discussions mean that livability includes a smart economy, smart living, a smart society, and smart governance in a smart city context. In other words, a livable city covers four of the six aspects of a smart city.

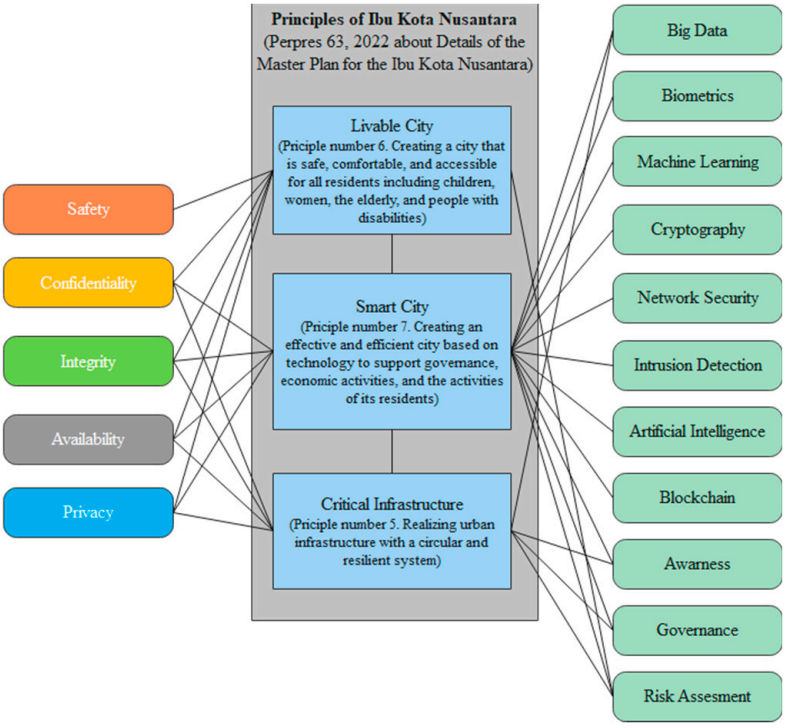

Figure 3. Relation of IKN Factors, Security Objective, and Technology.

The discussion on cybersecurity and human safety found a relationship between critical infrastructure and smart cities. The connectivity between infrastructure in smart cities and the involvement of information technology makes smart cities inseparable from critical infrastructure or, more specifically, critical information infrastructure. In the end, critical infrastructure exists in every dimension of a smart city because, in a smart city, the connectivity between service infrastructure is very high.

The literature review also confirmed the objective of information security, as stated in ISO 27001:2022, as a cybersecurity objective. Those cybersecurity objectives are confidentiality, integrity, and availability. In addition, the analysis also found privacy and safety, so overall, there are five cybersecurity goals in IKN, namely confidentiality, integrity, availability, privacy, and safety. ISO 27001:2022 also mentions other possible security objectives and several other possible objectives. Privacy and safety are not in the possibilities mentioned in ISO 27001:2022, but by using the existing looseness of definitions, privacy and safety are grouped under security objectives.

As for technology used in IKN cybersecurity, all cybersecurity technology is used in smart cities, while securing critical infrastructure is more about the cybersecurity management of big data. An analysis of IKN's factors found that livable cities and critical infrastructure are part of a smart city. That is why the mapping of security technology shows that more research is needed on the smart city aspect. Cybersecurity in critical infrastructure is more about security management through security governance, risk assessment, and security awareness. Identification, management, and education about the importance of securing critical infrastructure are necessary. Still, when implementing security, the technology used differs from other cybersecurity technologies in smart cities.

Although only two pieces of literature discuss livable cities with risk assessment of the technology, livable cities cannot be eliminated because this is part of the IKN development principles. Moreover, based on the literature, there is a link between livable cities and smart cities. Therefore, as shown in Figure 4, cybersecurity in IKN is implemented by seeing IKN as a smart city, a livable city, and having critical infrastructure to ensure confidentiality, integrity, availability, privacy, and safety by using existing security technology.

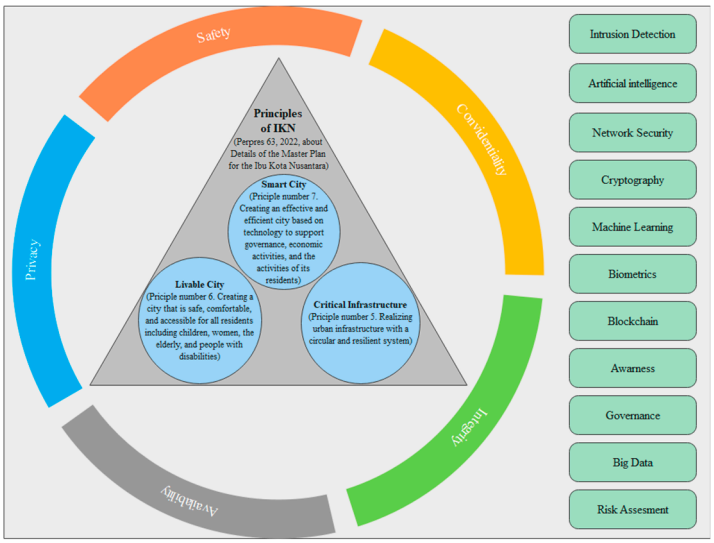

Figure 4. Proposed Framework.

We then interviewed the three experts to have them validate the cybersecurity framework. The three experts represent the National Cyber and Crypto Agency (the organization in charge of cybersecurity in Indonesia), practitioners whose role is to prepare smart city master plans, and academics in the field of information security. From the interview, all the experts agreed on three of the eight principles for IKN development related to cybersecurity and the concepts of a livable city, a smart city, and critical infrastructure. Until now, the development of Indonesia's new capital city has been conducted based on document Perpres 63, "The Detail Masterplan for the Ibu Kota Nusantara". Based on that document, at the very least, cyber security can be linked to development principles 5, 6, and 7. There is also a suggestion to use a standard cybersecurity framework such as NIST, but the proposed framework complements the NIST framework by adding privacy as a security objective.

The results of the interviews also recommend further researching the possibilities of three sub-security objectives: accountability, authentication, and auditability. These three security objectives can be described as support for confidentiality, integrity, and availability. For example, confidentiality can be achieved by maintaining authentication and auditability, and integrity is supported by accountability. The authentication method supports a variety of data secrecy methods in a system. Auditability and accountability will be used in case of a confidentiality or integrity breach.

From the validation process, all experts agreed to define the proposed technology on the framework as the latest technology in cybersecurity. This technology can be replaced by a new one in the future. These proposed technologies are implemented as a list of security technologies standardized by Indonesian cybersecurity institutions. After determining that cybersecurity technology in IKN is related to livable cities, smart cities, and critical infrastructure, the specified security technologies can continue to develop according to threat trends and developments in information technology.

5. Conclusions

The initial cybersecurity framework for IKN focuses on it being a smart city and livable city and its critical infrastructure. Identified factors are in line with the 5th, 6th, and 7th of the IKN development principles. The initial proposed framework is designed to preserve confidentiality, integrity, availability, safety, and privacy. To support the achievement of cybersecurity objectives, it is recommended to use big data, blockchain, biometrics, machine learning, cryptography, network security, artificial intelligence, and intruder detection. IKN cybersecurity also needs risk assessment, security governance, and security awareness so that the selected security technology can achieve the expected goals.

This research used smart cities, livable cities, and critical infrastructure as replacement concepts for the "Ibu Kota Nusantara", or the new capital city of Indonesia. This concept can also be used in other studies, noting that the phrases "Ibu Kota Nusantara", IKN, and new capital city that are not commonly used in scientific articles.

According to the Economist Intelligence Unit, there is a more detailed description regarding the livable city, but there are limitations to research related to the livable city assessment matrix. Therefore, future research can be carried out by further analysis using the referenced assessment matrix or building a custom livability assessment index. Furthermore, cybersecurity keywords in the literature search also limit the information obtained regarding technology trends. In addition, studies for the security of the new capital city of Indonesia should also be conducted relating to smart city security or critical infrastructure security technology.

Author Contributions: Methodology, P.A.W.P.; Supervision, D.I.S., R.R. and W.D.S.; Writing—original draft, D.I.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Indonesian Collaborative Research Program 2022 from Universitas Indonesia, contract number NKB 1071/UN2.RST/HKP.05.00/2022.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Pemerintah Indones. Undang-Undang Republik Indonesia Nomor 3 Tahun 2022 Tentang Ibu Kota Negara. 2022. Available online: https://www.presidenri.go.id/ (accessed on 13 October 2022).
2. Presiden Republik Indonesia. Peraturan Presiden Republik Indonesia Nomor 63 Tahun 2022 Tentang Perincian Rencana Induk Ibu Kota Nusantara. 2022. Available online: https://www.presidenri.go.id/ (accessed on 1 November 2022).
3. Bailes, A.J.K. *Business and Security Public—Private Sector Relationships*; Stockholm International Peace Research Institute: Solna, Sweden, 2004.
4. Lin, H.; Bergmann, N.W. IoT Privacy and Security Challenges for Smart Home Environments. *Information* **2016**, *7*, 44. [CrossRef]
5. Economist Intelligence. The Global Liveability Index 2022. Available online: https://www.eiu.com/n/campaigns/global-liveability-index-2022/?utm_medium=website&utm_source=archdaily.com (accessed on 1 November 2022).
6. Pemerintah Republik Indonesia. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik. Media Huk 110. 2018. Available online: https://www.presidenri.go.id/ (accessed on 12 October 2022).

7. Maja, P.W.; Meyer, J.; Von Solms, S. Development of Smart Rural Village Indicators in Line With Industry 4.0. *IEEE Access* **2020**, *8*, 152017–152033. [CrossRef]
8. Ceballos, G.R.; Larios, V.M. A model to promote citizen driven government in a smart city: Use case at GDL smart city. In Proceedings of the IEEE 2nd Int Smart Cities Conf Improv Citizens Qual Life, ISC2 2016, Trento, Italy, 12–15 September 2016. [CrossRef]
9. Ukwandu, E.; Ben-Farah, M.A.; Hindy, H.; Bures, M.; Atkinson, R.; Tachtatzis, C.; Andonovic, I.; Bellekens, X. Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends. *Information* **2022**, *13*, 146. [CrossRef]
10. Andrew, M.; Rashid, A.; Chivers, H.; Schneider, S.; Lupu, E.; Danezis, G. *The Cyber Security Body of Knowledge*; University of Bristol: Bristol, UK, 2021; p. 22.
11. ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection. In *ISO/IEC 27032: 2012 Information Technology—Security Techniques—Guidelines for Cybersecurity*; International Electrotechnical Commission (IEC): Geneva, Switzerland, 2012.
12. Kitchenham, B.; Pretorius, R.; Budgen, D.; Brereton, O.P.; Turner, M.; Niazi, M.; Linkman, S. Systematic literature reviews in software engineering—A tertiary study. *Inf. Softw. Technol.* **2010**, *52*, 792–805. [CrossRef]
13. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *Syst. Rev.* **2021**, *88*, 105906.
14. Kitchenham, B.A.; Madeyski, L.; Budgen, D. SEGRESS: Software Engineering Guidelines for REporting Secondary Studies. *IEEE Trans. Softw. Eng.* **2022**, *1*, 1. [CrossRef]
15. Penmetsa, M.K.K.; Bruque-Camara, S. A framework for building a sustainable digital nation: Essential elements and challenges. *Digit. Policy Regul. Gov.* **2021**, *23*, 262–286. [CrossRef]
16. Dai, X.; Yao, L. A classification method and implementation of Trojan and BotNet infected user based on threat matrix model. In Proceedings of the 2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), Leicester, UK, 19–23 August 2019; pp. 1231–1236.
17. Gamec, J.; Basan, E.; Basan, A.; Nekrasov, A.; Fidge, C.; Sushkin, N. An Adaptive Protection System for Sensor Networks Based on Analysis of Neighboring Nodes. *Sensors* **2021**, *21*, 6116. [CrossRef] [PubMed]
18. Himdi, T.; Ishaque, M.; Ahmed, J. Cybersecurity challenges during pandemic in smart cities. In Proceedings of the 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 17–19 March 2021; Institute of Electrical and Electronics Engineers Inc., Jeddah International College, Department of Computer Science: Jeddah, Saudi Arabia, 2021; pp. 445–449.
19. Yan, C.; Huang, Z.; Ke, C.; Xie, J.; Wang, J. A topology-aware access control model for collaborative cyber-physical spaces: Specification and verification. *Comput. Secur.* **2019**, *87*, 101478.
20. Tommaso, Z.; Ceccarelli, A.; Mori, M. A tool for evolutionary threat analysis of smart grids. In *Smart Grid Inspired Future Technologies*; Springer: Cham, Switzerland, 2017; Volume 203, pp. 205–211.
21. Duan, Y.; Lu, Z.; Zhou, Z.; Sun, X.; Wu, J. Data Privacy Protection for Edge Computing of Smart City in a DIKW Architecture. *Eng. Appl. Artif. Intell.* **2019**, *81*, 323–335. [CrossRef]
22. Kertis, T.; Prochazkova, D. Cyber curity of usenderground railway system operation. In Proceedings of the 2017 Smart City Symposium Prague (SCSP), SCSP 2017, Prague, Czech Republic, 25–26 May 2017; pp. 1–6.
23. Lupton, B.; Zappe, M.; Thom, J.; Sengupta, S.; Feil-Seifer, D. Analysis and Prevention of Security Vulnerabilities in a Smart City. In Proceedings of the 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 26–29 January 2022; pp. 702–708.
24. Lim, M.K.; Xiong, W.; Lei, Z. Theory, supporting technology and application analysis of cloud manufacturing: A systematic and comprehensive literature review. *Ind. Manag. Data Syst.* **2020**, *120*, 1585–1614. [CrossRef]
25. *ISO/IEC 27001:2022*; Information Security, Cybersecurity and Privacy Protection-Information Security Management System-Requirements. International Electrotechnical Commission (IEC): Geneva, Switzerland, 2022.
26. Kiss-Leizer, G.K. Environmental safety and living in a smart city. *Interdiscip. Descr. Complex Syst.* **2020**, *18*, 360–368. [CrossRef]
27. Appio, F.P.; Lima, M.; Paroutis, S. Understanding Smart Cities: Innovation ecosystems, technological advancements, and societal challenges. *Technol. Soc. Chang.* **2019**, *142*, 1–14. [CrossRef]
28. Espada, R.; Apan, A.; McDougall, K. Vulnerability assessment of urban community and critical infrastructures for integrated flood risk management and climate adaptation strategies. *Int. J. Disaster Resil. Built Environ.* **2017**, *8*, 375–411. [CrossRef]
29. Erastus, L.; Jere, N.; Shava, F.B. Secure Information Infrastructure Framework Components for a Smart City: A Case Study of Windhoek. In Proceedings of the 2020 IST-Africa Conference (IST-Africa), Kampala, Uganda, 18–22 May 2020; Institute of Electrical and Electronics Engineers Inc.: New York, NY, USA, 2020; pp. 1–10.
30. Malatji, M.; Marnewick, A.L.; von Solms, S. Cybersecurity capabilities for critical infrastructure resilience. *Inf. Comput. Secur.* **2021**, *30*, 255–279. [CrossRef]
31. Tse, D.; Li, R.; Zheng, H. Risks facing smart city information security in Hangzhou. In Proceedings of the 2019 3rd International Conference on Software and e-Business, Tokyo, Japan, 9–11 December 2019; pp. 29–33.
32. Vitunskaite, M.; He, Y.; Brandstetter, T.; Janicke, H. Smart cities and cyber security: Are we there yet?A comparative study on the role of standards, third party risk management and security ownership. *Comput. Secur.* **2019**, *83*, 313–331. [CrossRef]

33. Cui, L.; Xie, G.; Qu, Y.; Gao, L.; Yang, Y. Security and Privacy in Smart Cities: Challenges and Opportunities. *IEEE Access* **2018**, *6*, 46134–46145. [CrossRef]
34. Braun, T.; Fung, B.C.; Iqbal, F.; Shah, B. Security and privacy challenges in smart cities. *Sustain. Cities Soc.* **2018**, *39*, 499–507. [CrossRef]
35. Shukla, M.; Johnson, S.D.; Jones, P. Does the NIS implementation strategy effectively address cyber security risks in the UK? In Proceedings of the 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Oxford, UK, 3–4 June 2019; pp. 1–11.
36. Hasbini, M.A.; Eldabi, T.; Aldallal, A. Investigating the information security management role in smart city organisations. *World J. Entrep. Manag. Sustain. Dev.* **2018**, *14*, 86–98. [CrossRef]
37. Kumar, P.M.; Rawal, B.; Gao, J. Blockchain-enabled Privacy Preserving of IoT Data for Sustainable Smart Cities using Machine Learning. In Proceedings of the 2022 14th International Conference on COMmunication Systems & NETworkS (COMSNETS), Bangalore, India, 4–8 January 2022; Institute of Electrical and Electronics Engineers Inc.: New York, NY, USA, 2022; pp. 1–6.
38. Esposito, C.; Ficco, M.; Gupta, B.B. Blockchain-based authentication and authorization for smart city applications. *Inf. Process. Manag.* **2020**, *58*, 102468. [CrossRef]
39. Sengupta, N. Designing cyber security system for smart cities. In *Smart Cities Symposium*; Institution of Engineering and Technology, Department of IT, University College of Bahrain: Manama, Bahrain, 2018; pp. 1–6.
40. Mohammad, R.M.A.; Abdulqader, M.M. Exploring cyber security measures in smart cities. In Proceedings of the 2020 21st International Arab Conference on Information Technology (ACIT), Giza, Egypt, 28–30 November 2020; Institute of Electrical and Electronics Engineers Inc., College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, Department of Computer Information Systems: Dammam, Saudi Arabia, 2020; pp. 1–7.
41. Alromaihi, S.; Elmedany, W.; Balakrishna, C. Cyber security challenges of deploying IoT in smart cities for healthcare applications. In Proceedings of the 2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Barcelona, Spain, 6–8 August 2018; pp. 140–145.
42. Elsaeidy, A.; Elgendi, I.; Munasinghe, K.S.; Sharma, D.; Jamalipour, A. A smart city cyber security platform for narrowband networks. In Proceedings of the 2017 27th International Telecommunication Networks and Applications Conference (ITNAC), Melbourne, VIC, Australia, 22–24 November 2017; pp. 1–6.