future internet

MDPI

Review

Information Security Applications in Smart Cities: A Bibliometric Analysis of Emerging Research

Thiago Poleto [1,*], Thyago Celso Cavalcante Nepomuceno [2], Victor Diogho Heuer de Carvalho [3,*], Ligiane Cristina Braga de Oliveira Friaes [1], Rodrigo Cleiton Paiva de Oliveira [1] and Ciro José Jardim Figueiredo [4]

1 Department of Business Administration, Institute for Applied Social Sciences, Federal University of Pará, Belém 66075-110, Brazil; ligianebraga@ufpa.br (L.C.B.d.O.F.); ro.wright09@gmail.com (R.C.P.d.O.)
2 Department of Statistics, Center for Exact and Natural Sciences, Federal University of Pernambuco, Recife 50670-901, Brazil; thyago.nepomuceno@ufpe.br
3 Technologies Axis, Campus do Sertão, Federal University of Alagoas, Delmiro Gouveia 57480-000, Brazil
4 Department of Engineering, Campus Angicos, Federal Rural University of Semi-Arid, Angicos 59515-000, Brazil; ciro.figueiredo@ufersa.edu.br
* Correspondence: thiagopoleto@ufpa.br (T.P.); victor.carvalho@delmiro.ufal.br (V.D.H.d.C.)

Abstract: This paper aims to analyze the intellectual structure and research fronts in application information security in smart cities to identify research boundaries, trends, and new opportunities in the area. It applies bibliometric analyses to identify the main authors and their influences on information security and the smart city area. Moreover, this analysis focuses on journals indexed in Scopus databases. The results indicate that there is an opportunity for further advances in the adoption of information security policies in government institutions. Moreover, the production indicators presented herein are useful for the planning and implementation of information security policies and the knowledge of the scientific community about smart cities. The bibliometric analysis provides support for the visualization of the leading research technical collaboration networks among authors, co-authors, countries, and research areas. The methodology offers a broader view of the application information security in smart city areas and makes it possible to assist new research that may contribute to further advances. The smart cities topic has been receiving much attention in recent years, but to the best of our knowledge, there is no research on reporting new possibilities for advances. Therefore, this article may contribute to an emerging body of literature that explores the nature of application information security and smart cities research productivity to assist researchers in better understanding the current emerging of the area.

Keywords: information security; smart city; technical collaborations networks; applications; bibliometric analysis

Citation: Poleto, T.; Nepomuceno, T.C.C.; de Carvalho, V.D.H.; Friaes, L.C.B.d.O.; de Oliveira, R.C.P.; Figueiredo, C.J.J. Information Security Applications in Smart Cities: A Bibliometric Analysis of Emerging Research. *Future Internet* **2023**, *15*, 393. https://doi.org/10.3390/fi15120393

Academic Editor: Francesco Buccafurri

Received: 18 October 2023
Revised: 4 November 2023
Accepted: 7 November 2023
Published: 1 December 2023

1. Introduction

The advancement of solutions and tools focused on information security for smart cities is gaining prominence worldwide [1–7]. Furthermore, there has been a noticeable increase in the production of large volumes of data, agility in information exchange, data analysis (Data Science), development of smart cities, and connectivity between various devices. These continuous interactions with internet-focused solutions (Internet of Things—IoT) must be conducted in compliance with regulations [8–10]. However, they concurrently introduce profound challenges, especially in terms of data governance, and there is a growing emphasis on safeguarding the integrity, confidentiality, and availability of data as it is generated, processed, and exchanged across diverse entities, spanning from private organizations to public sectors and the general populace [11–14].

As public services gravitate towards interconnected digital ecosystems, we can identify significant potential benefits, such as streamlined operations and bolstered resilience in

critical infrastructures. Nonetheless, for metropolises and regions striving to transition into the smart city paradigm, it is imperative to not only meticulously assess but also proactively mitigate the inherent cybersecurity risks stemming from such integration [13–21]. While no technology solution can guarantee complete security, communities need to implement smart city technologies while considering the need to balance efficiency, innovation, and cybersecurity [20,22–25].

This context demands promoting privacy protections, national security, and the secure operation of infrastructure systems. Cities should tailor best practices to their specific cybersecurity requirements, ensuring the protection of citizens' private data as well as the security of sensitive government and business information [20,24,26,27]. By promoting protection through proper guidelines, communities can strive to create a safe and secure environment while embracing the benefits of technological advancements [28].

In recent years, organizations have turned their attention to the increased risks that the lack of information security causes in the evolution and survival of businesses, mainly due to the large offer of technological devices and the growing access and dissemination of data and information [29–32]. The lack of information security evidence many losses for the different business stakeholders, especially when it negatively impacts the trust of customers and suppliers, the efficiency of services, the availability of operations, the credibility of the business, and the image of the company [33]. In this sense, organizations have adopted strategies to prevent the occurrence of security flaws caused by Denial of Service Attacks (DoS), hacking, malware, phishing, spoofing, ransomware, spamming, and other types of cyberattacks [31,34–37]. Strategies, in general, are adopted to protect the business performance and maintain operational efficiency at competitive levels [38]. Thus, excellence in the cybersecurity process is essential to ensure the integrity, availability, and confidentiality of business data and information [39,40].

The discussion over the importance of information security has been highlighted in recent literature. The advancement of research in the area has considered aspects from risk assessment to recovery and resilience of cybersecurity [41,42]. On many occasions, Information Technology (IT) managers seek to analyze solutions to conduct operational strategies aimed at protecting business [43]. In recent years, although many researchers [44–49] have presented approaches to the importance, investment, and contribution of cybersecurity to organizations, society, and government, there is still a gap in the current literature: there are no studies that analyze the most influential works in the area of cybersecurity with an integrated view.

In recent studies on smart cities, there is a growing interest in integrating innovative technologies to optimize urban management and improve the quality of life for citizens. However, upon reviewing the existing literature, a gap is identified in the systematic review related to information security applications in this context. While many studies address the benefits and potential implementations of these technologies, few delve deeply into specific solutions to ensure data protection and user privacy. Given the critical importance of information security in highly connected environments, such as smart cities, this gap presents an opportunity for researchers and IT professionals to delve deeper and contribute with insights and robust solutions to this emerging challenge.

One of the premises for understanding the application of information security in smart city research activities is to analyze its manifestation in the form of scientific production. In this sense, this paper aims to perform a bibliometric analysis to deepen knowledge of new applications of information security in smart cities to identify the main groups of researchers working collaboratively in the area. Moreover, this study provides a summary of research patterns based on an institutional network to present a better understanding of research advances and the latest content about information security in smart cities published in journals during the period from 2015 to 2023. The relevant articles were retrieved from the Scopus database.

The bibliometric analysis allows the visualization of the technical quality and impact of research, as well as grouping authors and co-authors, identifying the relationship

between studies through keywords and number of citations, and displaying intellectual contributions from research fields, among other analyses. In addition, solutions and review of smart cities opens many opportunities and scopes for open research.

This paper is structured as follows: Section 2 presents a theoretical reference with related works about smart cities and information security research; Section 3 is devoted to Materials and Methods; Section 4 presents the Findings and Discussion; Section 5 contributes to the theory and presents practical implications; the conclusion, limitations, and further research are provided in Section 6.

2. Smart Cities and Information Security

Before starting a discussion about papers that have reviewed the literature on smart cities, it is essential to address some concepts. A smart city is understood as an urban area where electronic sensor technology is used to collect data from devices as well as assets and citizens for analysis and processing of the data to manage and monitor public infrastructures [50,51]. Smart cities are characterized by the following characteristics in terms of digitalization: Internet of Things (IoT), Big Data, and Cloud Services to promote integration [52,53].

At the heart of a smart city lies a tapestry of devices interconnected via wireless networks, often operating on open network protocols or APIs [54–56]. These elements, by their very design, can be susceptible to breaches, even by the smallest snippets of malicious code [57–59]. Consequently, information security shifts beyond the individual user's realm and emerges as a communal imperative within the smart city landscape [60–62]. Moreover, the escalating intricacy of the system's network infrastructures, magnified by digital communication, interconnected devices, and diverse network architectures, inevitably poses heightened security challenges [1,63–67].

The consequences of successful cyberattacks against smart cities can be severe and wide-ranging. They may include disruptions to essential infrastructure services, substantial financial losses, exposure of citizens' private data, erosion of trust in smart systems, and even physical harm or loss of life due to impacts on physical infrastructure. According to Shin et al. [68], global spending on cybersecurity hardware, software, and services has significantly grown in the past few years, and the annual cybersecurity investment averages USD 1 billion by some financial and tech companies. Cyberattacks are a serious threat to the successful implementation of smart cities-related services. Comprehensive security mechanisms and a security-oriented mindset throughout the entire organization are essential to avert and control this risk.

Table 1 presents the risk domain in information security to smart cities found in the literature, addressing different perspectives on provider and user application of technologies. Upon examination of the table, it is evident that the identified domains encompass topics that resonate with the discussions conducted by experts in the literature, as well as those on Cloud computing, IoT, data interpretation, and smartphone devices. Moreover, the highlighted risks emphasize the imperative need for acquiring deeper insights in advance, specifically in the realm of information security within smart cities, a domain that is growing in significance. Nonetheless, it is worth acknowledging a potential drawback associated with the abundance of published material, which serves as a catalyst for conducting the systematic review presented in this paper to identify guidelines that serve as a contribution to the theme.

The analysis of these works allows us to conclude that information security risk in smart cities is still in the development stage in different devices. Thus, more comprehensive and complete research and analysis of all recent publications in the field of information security is necessary and still lacking. In this sense, a bibliometric study is a valuable tool to present the interrelationships of researchers, their contributions, and the gaps to be worked on.

Table 1. Main detected information security risk domains according to literature.

Area	Risk Domain	References
Cloud computing (platform of services over the internet, accessible by people and business companies)	Cloud threats	[69–72]
	Custodianship of keys	[73]
	Security of data	[60,74–77]
	Security attacks	[75,78–85]
	Lack of a data privacy policy	[73,77,86–92]
Internet of Things (concerning devices that have an internet connection and that can communicate with the network independently of human action).	Attacks on IoT devices	[9,35,83,87,93–96]
	Lack of effective access controls	[89,97–104]
	Protecting sensitive data	[32,105–107]
	Botnet activities	[35,108–110]
	Privileged user access	[89,99,111]
Data interpretation (essentially the representation of complex data and understand trends and follow patterns)	Security reports	[112–114]
	Discover sensitive data	[115–118]
	Errors and inconsistency Decision	[119–121]
	Privacy violations	[122–126]
Smartphones (smart communication mobile devices)	Security of data	[127–130]
	Smartphone threats	[131,132]
	Protecting sensitive data	[133]
	Lack of privacy of stakeholders	[134,135]

Related Reviews

The literature on topics associated with information security, cybersecurity, and smart cities contains some systematic literature reviews with very interesting content to assist researchers and practitioners in their definitions in favor of new research and related practical developments. The swift progress of artificial intelligence and data-driven technologies has opened new avenues for tackling intricate socioeconomic issues in the modern world through the utilization of diverse datasets and the application of advanced analytical techniques, fostering inclusive development and sustainable growth in smart cities [136].

The topic of cybersecurity has been a growing concern in scientific literature that extends and is interlinked with many social issues. In the comprehensive review of applications in public security by de Carvalho and Costa [137] spanning materials published between 2014 and the first half of 2021 across significant bibliographic databases like Scopus, Web of Science, IEEE Xplore, and ACM Digital Library, the authors highlight the adaptive techniques and mining techniques to enhance pirate software detection and other security-related concerns.

Following, we present a set of seven systematic reviews related to the one presented in this document, retrieved from the Scopus database. This set was selected based on its impact, measured based on the number of citations.

Habibzadeh et al. [40] developed a survey that provides an overview of both the theoretical and practical challenges and opportunities, considering not only their technical dimensions but also addressing policy and governance concerns. Their study underscores the need for collaborative efforts among different stakeholders to achieve sustainable and secure smart city ecosystems. It offers a comprehensive examination, discussing security and safety implications for critical infrastructures and the resulting policy considerations at various levels. It also assesses privacy and security vulnerabilities inherent in smart city architecture, along with a focus on common smart city applications.

The survey by Sanchez et al. [138] explored the recent advancements in the field of device behavior fingerprinting, examining its applications, sources of behavioral data, and

the techniques employed for processing and assessment. The reliability and performance of emerging environments such as smart cities, Industry 4.0, and crowdsensing depend on the proper functioning of fingerprint devices. This entails a comprehensive grasp of the capabilities of these devices, including sensors and actuators, and the capability to identify potential irregularities arising from cyberattacks, system failures, or misconfigurations.

The survey by Jimada-Ojuolape and Teh [139] provides a comprehensive review of research that extends beyond assessing reliability at the component level and takes into consideration the influence of Information and communication technology integrations on the overall system reliability. The study presents some recommendations based on the literature, which are based on either the adequacy aspect or the security aspect of reliability. It also presents some technological challenges to the reliability of smart grids, going from Infrastructure failures due to cyber–physical interdependencies, passing through environmental aspects, such as the weather conditions, reaching combatting cybersecurity vulnerabilities, such as intrusions/infiltrations.

Kim et al. [140] conducted a systematic and comprehensive investigation of autonomous vehicles by analyzing 151 papers published between 2008 and 2019. They categorized autonomous attacks into three main groups: those targeting the autonomous control system, components of autonomous driving systems, and vehicle-to-everything communications. Protection against these attacks was categorized into security architecture, intrusion detection, and anomaly detection. With advancements in big data and communication technologies, there is a gradual evolution of techniques that employ artificial intelligence and machine learning for anomaly detection. Their survey suggests that future research in autonomous attacks and defenses should be closely integrated with artificial intelligence, as it constitutes a critical component of smart cities.

Alotaibi and Barnawi [141] present a thorough examination of security considerations for massive Internet of Things (IoT) within the context of 6G networks, with a particular focus on Intrusion Detection Systems (IDS). The authors claim this is the inaugural survey to encompass the amalgamation of Machine Learning (ML), Deep Learning (DL), and essential networking technologies that underpin the forthcoming 6G infrastructure for securing massive IoT. As future trends for 6G, they highlight self-adaptive intrusion detection systems, the use of federated learning, self-supervised learning, quantum machine learning, explainable artificial intelligence, transfer learning, and big data technologies, supporting the development of intelligent protection platforms.

Raimundo and Rosário [142] examined the prevailing literature trends concerning the opportunities and threats in Industrial Internet of Things (IIoT) cybersecurity. They have reviewed 70 pivotal articles identified through an extensive survey of the Scopus database, intending to outline the ongoing discourse surrounding IIoT rather than proposing specific technical remedies for network security issues. The study highlighted key themes in the current debate on the involved topics, considering: (i) a cybersecurity axis, observing platforms that may accommodate smart objects, issues related to smart grids in IoT-controlled environments, critical technologies, best practices, policies, and frameworks; (ii) a machine learning axis, to encompass artificial intelligence techniques in cybersecurity; (iii) an IoT axis that considers the use of artificial intelligence combined to physical devices supporting cybersecurity measures for systems protection; (iv) an Industry 4.0 (or IIoT) axis covering industrial applications of IoT and artificial intelligence, also demanding concern about the security of the systems involved; and (v) blockchain and cloud computing axis, representing the decentralized architectures needed to run all the previous concepts plans and technologies.

Yang et al. [143] developed a systematic overview of research related to these technologies, which includes four key components. First, they present a summary of urban sensor concepts and applications. Second, they analyze the progress in multisource heterogeneous urban sensor access technologies, encompassing communication protocols, data transmission formats, access standards, access technologies, and data transmission methods. Third, they review data management technologies for urban sensors, focusing on data cleaning,

data compression, data storage, data indexing, and data querying. Fourth, they address challenges associated with these technologies and propose viable solutions, specifically in the realms of integrating massive Internet of Things (IoT), managing computational load, optimizing energy consumption, and enhancing cybersecurity. Finally, the paper concludes by summarizing their work and hinting at potential future development directions.

3. Materials and Method

The bibliometric analysis uses statistical methods to evaluate the evolution of a particular research area. In this sense, it is possible to (i) evaluate the number of publications, the level of quality, the impact, and the contribution of the results; (ii) to carry out a mapping of the scientific activities of the authors; (iii) to understand networks of citations based on the authors; (iv) to obtain a real and detailed visualization of the results and intellectual structures of a scientific domain; (v) to promote the construction of knowledge; (vi) to monitor the evolution of a research field and (vii) to clarify unexplored research topics.

In the past ten years, the advance of cybersecurity research has developed significantly by influential authors in different journals and research areas. The present study consists of a technical and structured analysis of the progress of literature on cybersecurity, with the objectives of presenting collaborations in the editorial production of researchers, highlighting new insights on the role of information security engineering in the world, and stimulating development on future research lines. To direct the research, some questions are posed:

- *Q1—What are the patterns of information security applications found in research on smart cities?*
- *Q2—What are the most demanding areas for information security in smart cities studies?*
- *Q3—What research has the most influence on the application of information security in smart cities?*

To answer these questions, this study adopts a theoretical approach, aiming to understand the state-of-the-art information security and smart cities research fields through bibliometrics and content analysis. Figure 1 shows the research design used in this paper, which consists of five steps.

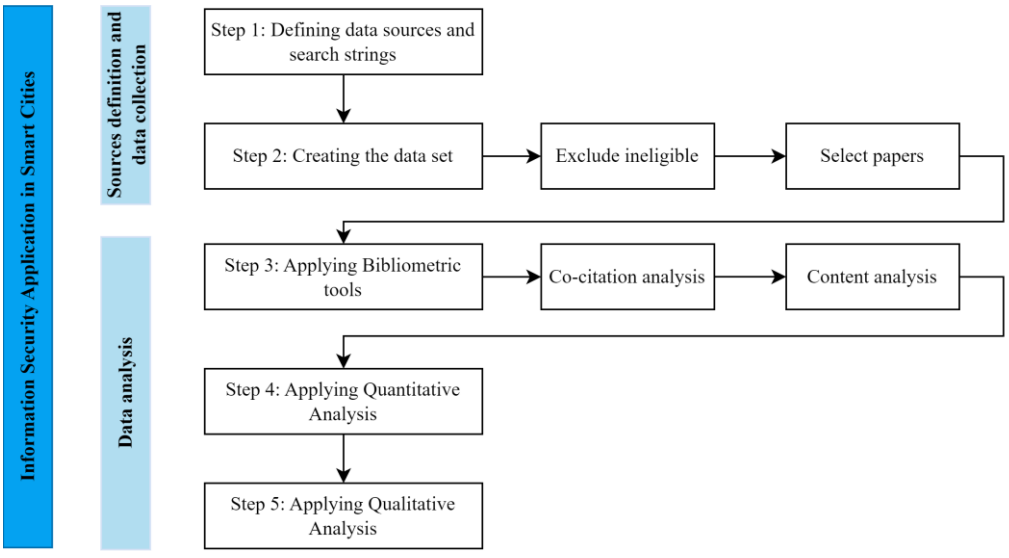

Figure 1. Research design.

Step 1 starts with the data sources definition, considering the Scopus database, followed by search string creation. In this study, two combinations of keywords were defined to compose the search string: (I) "information security" and "smart city"; and (II) "cyberattacks" and "smart city". These terms are broad and expand the knowledge about

the different knowledge application areas of the theme. The search was applied to titles, abstracts, and keywords of complete published articles.

In Step 2, the dataset consists of complete articles published in journals indexed in Scopus, ranging from 2015 to 2023. We decided to start searching for published results from 2015 due to the high number of citations from one of the articles of greater relevance to the area, published in the same year.

The work entitled "Cyber security challenges in smart cities: Safety, security and privacy", indicated in the reference list, has obtained 650 citations to date [15]. For this reason, we consider this time interval as the most relevant to collect data. A filter was used to remove articles that emerged from books, categorized. The purpose of using this filter was to focus on the article and conference reviews with significant academic impact and relevance in the research platform. In addition, other categories of publications have also been removed, so the objective is to identify the sectors and fields in which there are one or more surveys and the sectors and methods in which there are no surveys available. The Scopus database was selected due to the broad approach of indexed sources among journals, conferences, and books, increasing the range of data collection for the bibliometrics analyses.

As shown in Figure 2, there is a significant increase in articles on information security and smart cities. The search results returned a total of 1978 articles, including conference papers (55.5%) and journal articles (44.5%).

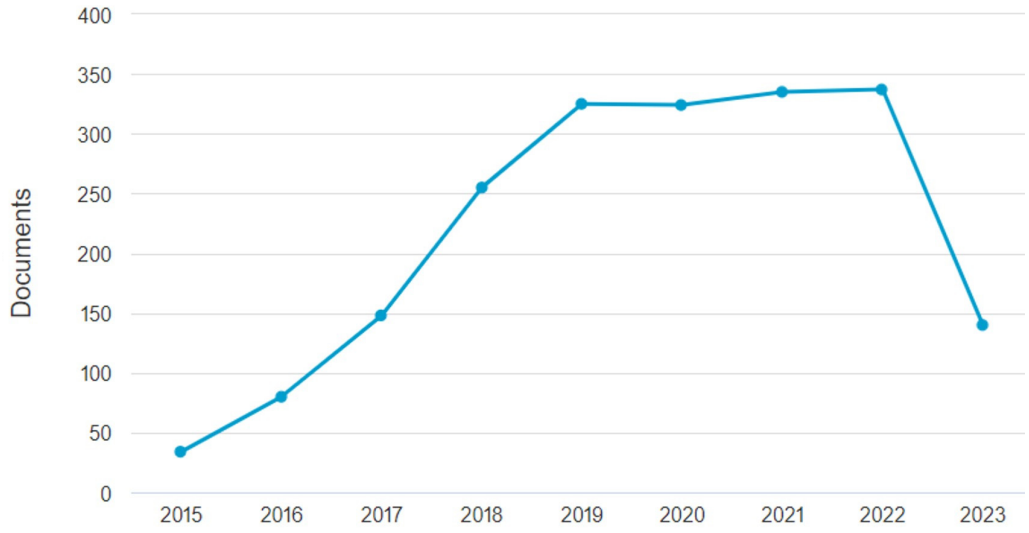

Figure 2. Trend line based on the number of publications by year in the field of information security in smart cities.

In Step 3, the VOSViewer software [144], which is a text-mining tool that supports comprehensive and useful compilation of metadata, supporting data generation, and graph visualization, was used as a bibliometric analysis tool.

In Step 4, the quantitative analysis involved the implementation of statistical, network, and content methods through the development of descriptive and cluster analyses comprising information regarding articles, journals, authors, citations, references, and keywords in terms of annual progress in the field of cybersecurity research. The objective was to discover the implications of quantitative results in terms of the historical development of the application of information security and smart cities research field, its patterns, and evolution to answer the three research questions.

Finally, in Step 5, qualitative analysis was used to investigate production indicators (most productive authors, number of publications, types of authorship, area of training), the international authors who constitute the research interface in the area or related areas, and the information security and smart cities community. Also, the analysis of citations and their different relationships contributed to the identification of epistemological, methodological,

and theoretical influences in the domain investigated. From this, through distinctive classifications and thesaurus, the universe of articles analyzed was categorized, which allowed identifying the gaps regarding the study object and contributing to improving the representation schemes on smart cities knowledge.

4. Findings and Discussion

The advancement of IT and the emergence and growth of the internet led organizations to adopt new business models based on the potential market focused on creating and using cyberspace information. This business model allows organizations to obtain advantages, but on the other hand, they need to face several problems related to cyberspace security management, which are currently quite prominent.

The first publication in the area is "Cyberspace Security Management," published in 1999 by Chou et al. [145] in the journal of Industrial Management and Data Systems. This first publication evidences the leading causes of Internet security incidents. It starts the discussion about real concerns involving inherent risks, technology weaknesses, policy weaknesses, unauthorized intruders, and legal issues often provoked by players, which affect several business and government organizations in cyberspace. Chou et al. define the users, business sectors, and regulatory agents as leading players that influence the evolution of business and can interfere with principles of cybersecurity, such as confidentiality, integrity, and availability of data and information. The contributions of Chou et al. encourage the development of discussions on potential techniques, methodologies, and investment in IT solutions that address issues related to cybersecurity. As a result, several authors developed studies associated with the area and presented the results of a significant impact on the literature. Therefore, an analytical study of the main trends in the field, discussed in recent years, is suitable.

4.1. Identifying the Information Security Applications in Smart Cities Clusters of Research through Bibliographic

To analyze and visualize the knowledge clusters of research on information security applications in smart cities, the graph of relation in Figure 3 was created, considering the authors' groups according to application theme.

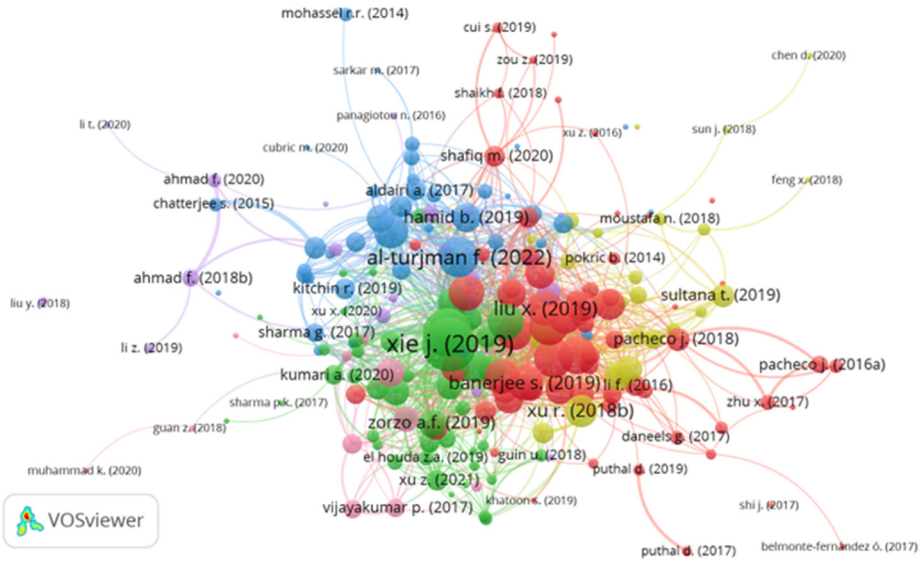

Figure 3. Clusters of authors according to applications about information security in smart cities.

The depiction of inter-publication relationships is facilitated by the quantity of links and the spatial proximity of nodes within the visual representation of Figure 3. Each node (circle) on the map corresponds to a publication, and the size within this visualiza-

tion is indicative of the volume of citations received by a respective publication. Proximity in the visualization denotes a stronger correlation, as determined by co-citation patterns, be-tween publications situated closely compared to those positioned at a greater distance [137,146–149]. The linkages between nodes serve to elucidate co-occurrence relationships, with closely associated term clusters forming tightly coupled groups [146,149]. This ap-plication of VOSviewer's co-occurrence analysis emerges as a robust method for constructing conceptual maps, enabling the identification of pivotal ideas and themes within a dataset and facilitating the visual representation of their interconnections in an accessible manner [147,149].

Table 2 details the cluster's compositions, separating them by name (related to the application domain) and listing their sizes as well as the most representative articles.

Table 2. Cluster identification with related domain, size, and most representative articles.

Cluster Number/Color	Cluster Name	Size	Representative Articles
Cluster 1/Red	Smart Power Grid in Smart Cities	324	[3,55,71,83,99,111,150–215]
Cluster 2/Green	Authentication in Smart Cities	241	[22,51,63,85,91,93,94,166,216–272]
Cluster 3/Blue	Cyberattacks in Smart Cities	153	[1,4,273–293]
Cluster 4/Yellow	Security platforms for Smart cities	121	[60,294–309]
Cluster 5/Pink	Evaluation of threats to cybersecurity	99	[6,54,310–324]
Cluster 6/Purple	Cybersecurity and society	78	[325–334]

Following, a description of each cluster is provided.

4.1.1. Cluster 1 (Red): Smart Power Grid in Smart Cities

One of the applications of information security is related to smart power grid maintenance in smart cities. A smart power grid can offer support to a smart communications grid since society increasingly requires information transfer infrastructure in daily activities [65]. Over the years, utilities have invested in communication networks to improve awareness of the power grid assets and to control, automate, and integrate the service delivery systems. The key point of integrating systems and working in real-time is connectivity. Most of the time, the web facilitates systems integration and benefits society with this support.

On the other hand, the web environment allows targeted attacks and attempts to break into the system. The North American Electric Reliability Corporation [335] highlighted compliance concerns in strengthening essential cybersecurity across the entire power system and emphasized that this requires a series of cybersecurity concerns [87,88,336,337].

For some authors, the smart grid needs to be observed and measured before being controlled and automated [338]. To that end, the automation of the power substation helps utilities add sophisticated protection and control functions while offering more visibility into the performance and integrity of the network infrastructure. Also, it is essential to note that the resilience of physical and electrical networks must also be improved according to the flow of information, as critical operations can cause failures or can be combined with physical attacks to create a blackout [339].

A reliable smart grid requires layered protection applications that consist of a cybernetic infrastructure that limits adversary access and limits the operation of the transmission accurately during an attack.

4.1.2. Cluster 2 (Green): Authentication in Smart Cities

One of the mechanisms for protecting data and information is access control policies for systems. Access control helps to prevent unauthorized people from entering the virtual and/or physical environment and engaging in unauthorized behavior. By ensuring access control, the integrity of employees and service providers is provided, as well as the integrity of data and information [337].

Over the years, the growing number of companies that select an outsourcing strategy for managing the entire IT infrastructure has been noticed. This interest is often motivated by the high investment in current IT security solutions, which require constant adaptations to the environment [340]. On the other hand, this need for adjustments makes many outsourced companies assume that their technology service providers are responsible for data control. However, when it comes to information security and compliance, the organization promoting the leading service remains responsible for all the information it has, especially if the company wants to obtain more profitable results from the data.

In this context, the objective of managers is to ensure that the large volumes of data collected and stored by their organizations can be used as instruments that help to generate better business strategies, making companies more objective and eliminating any types of confusion that may be caused by the total amount of information to be evaluated, adopting control systems with different types of possibilities, which can be physical or digital [219,341].

4.1.3. Cluster 3 (Blue): Cyberattacks in Smart Cities

The popularization of cloud computing encouraged the development of new businesses and reduced the need for high investment in IT infrastructure for small businesses, in particular. On the other hand, cybersecurity has become a significant concern for these companies. In the virtual environment, attackers create different threats to the systems of different businesses, from financial services agencies to sizeable industrial control systems [252,342,343]. Attack methods vary widely, using simple techniques to exploit the vulnerabilities of access and communication protocols or through combined operations for the use of multiple web bots [344].

One of the strategies to combat these threats is intrusion detection, the most effective security mechanism for detecting internal attacks that consists of the process of monitoring and analyzing events that occur in a computer system or network in search of patterns of possible security incidents. For the authors, these security incidents are violations or threats to security policies defined as attempts to compromise the reliability, integrity, or availability of system resources [345–348]. Many types of malware can be programmed to destabilize the operation of a system, such as viruses, worms, Trojans, and backdoors [349,350].

One of the main concerns of the authors is that the automatic detection of known and unknown kernel rootkits on virtual machines is becoming an urgent problem. For the virtual environment, an Intrusion Prevention System (IPS) is considered an extension of the Intrusion Detection System (IDS) and can be executed when threats or malicious activities are detected [351]. Thus, there is a tendency for new solutions to be made available to promote a kind of digital investigation and detect cybercrimes [352].

4.1.4. Cluster 4 (Yellow): Security Platforms for Smart Cities

For current businesses, one of the main assets is useful information. However, defining the monetary value of threats to this information can be a complex process. Economic decision models have been used to quantify the cyberattack process or demonstrate the intruder's detailed behaviors [353,354]. The advances in this area are mainly based on structured ways to present the consequences of the inventions to the IT Manager and recommend viable actions to avoid possible theft of information, for example, which represent the highest external cost, followed by the costs associated with interrupting operations of business [355].

To deal with rapidly evolving threats and risks, different approaches can be used to perform the command injection attack on the cyber component in the SCADA system: Model of the SQL Injection Attack, Model of the Secure Sockets Layer (SSL), Model of the Address Resolution Protocol, Model of the Buffer Overflow Attack [64,356]. In this context, dealing with an analytical decision model under conditions of uncertainty can be important for IT managers when planning information security programs.

4.1.5. Cluster 5 (Pink): Evaluation of Threats to Cybersecurity

The domain of cybersecurity threats is directly related to discussions about cybersecurity control and data in online services. Form IT advancement, new communication technologies, and control methods may allow better regulation of the smart grid; however, they also introduce serious threats to cybersecurity. In the Digital Age, security is the keyword. For the authors, having reliable data, systems, and people is indisputable because cyberattacks happen frequently, and systems capable of preceding an attack are essential [357].

Cyberattacks may also cause cascading failures in a power system, thus posing a serious threat to national infrastructure. Because of this, the authors suggest that the preconditions for managing cybersecurity risks are discovering incidents, collecting data, and viewing that data [174,358]. Three principles support this management cycle: maintaining the right data, robust IT infrastructure (systems), and an appropriate scope of sharing (people).

Impact analysis of threats is necessary to analyze the consequences of interruptions in the flow to protect and enable the evolution of business through technology, as well as to monitor users, observe the behavior, and monitor the development of attacks. Therefore, making potential threats clear can improve the protection shield and allow for new business opportunities [341].

The idea of resilience against a cyberattack, in addition to helping to know how to deal with a situation for which companies are not prepared, is to recognize the complexity of a scenario and have a contingency plan and defenses at different levels of security. In this way, it is possible to mitigate possible impacts resulting from cyberattacks [359].

In this sense, performing defensive security planning is essential, as the systems will cease to function over time, generating large potential losses for companies. Hong et al. [360] comment that investing in business cybersecurity is essential, given that criminals focus on operating systems with security gaps that have not been fixed or that have not yet been updated to a newer version. This vulnerability increases the risk and highlights the importance of investing in a consistent monitoring process [361].

In several countries, cyber defense constitutes a national security framework in which states establish policies at all levels (public and private) to guarantee individual freedoms and to respond to aggressions and invasions by developing response and cooperation systems [362]. Taking these security policies as a reference related to cyber resilience, emerging countries can adopt the definition of tasks and missions to establish security standards in the public and private environment, highlighting the specific criticality of the IT infrastructure [363].

4.1.6. Cluster 6 (Purple): Cybersecurity and Society

One of the most recent discussions related to cybersecurity has involved the influence of social aspects applied to the advancement of IT solutions [364]. Given the increase in urbanization around the world, growing populations are overloading the social services provided by the government, which in turn aims to facilitate the processes that citizens trust and need. This aspect motivates the emergence of the concept related to the construction of functional cities, which allow residents to have happier and healthier lives in a smart environment. In so-called "cities of the future," communities and organizations make extensive use of information technology to ensure broad and efficient access to early childhood education programs, professional recycling, and other vital social and citizenship programs that can be digitally connected [365].

However, one of the central points of the discussion is that there is no human consensus on ethics, especially on the sharing of information and space. Ethics is interpreted as a concept applied to a given context and, therefore, extremely complex to be programmed [366]. For the authors, machines need to be programmed with the minimum ethics necessary to avoid consequences in the future, but when human ethics is assumed, it does not seem to be the best model for teaching machines [367]. This motivation stimulates the discussion

about new ethics, something close to the consensus that would be used to program the artificial intelligence of the future.

This cluster involves the relationship between cybersecurity incidents and understanding of human behavior, in particular, incidents registered in business environments. For the authors, the protection of confidential data in companies is fundamental for business development and allows risks to be minimized [366]. This protection is based on two factors: technical and human factors. In general, the functional element involves investing in IT solutions that ensure access control mechanisms, user identification, antivirus systems, and restricted access to components of the IT infrastructure. On the other hand, the human factor refers to the user's perception of information security related to the knowledge of vulnerabilities and severity of risk regarding the lack of corruption of data and information, information shared on the internet, practices, and experiences with information security in the business environment.

The relationship between these factors raises a relevant discussion for the development of protection strategies that ensure control over the influence of human behavior in detriment to the investment of technical factors [342]. Cybersecurity strategies can be developed based on the perception of human behavior in an integrated manner with specialized solutions and IT governance to monitor the movement of confidential data that can be transmitted outside the company. The destructive consequences of spills are clear, but the risks caused by the human factor are often overlooked and can cause a company to go bankrupt. A situation that can exemplify this loss is when a sales employee improperly uses customer data, being able to use private information regarding business transactions in an unworthy manner [366].

In this context, awareness must be an ongoing effort to educate employees about policies, threats to data and information security, and how to deal with them [368]. Protection Motivation Theory can be applied to understand and develop a culture that motivates employees to maintain safe practices in their daily lives and transform awareness training into something personal. In addition to these theories, educational games can help support the concepts of awareness and improve understanding of possible incidents and their impacts on the organization and its business [128].

4.2. Top Authors with the Highest Number of Citations

Table 3 presents the 20 highly cited articles in information security and smart cities in the Scopus database.

Table 3. The 20 most cited articles on information security and smart cities.

Index	Author	Total of Citations	Title	Reference
1	Farahani et al., 2018	1001	Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare	[155]
2	Rathore et al., 2016	996	Urban planning and building smart cities based on the Internet of Things using Big Data analytics	[54]
3	Dagher et al., 2018	746	Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology	[101]
4	Biswas et al., 2016	746	Securing smart cities Using Blockchain Technology	[369]
5	Elmaghraby et al., 2014	640	Cyber security challenges in smart cities: Safety, security and privacy	[15]

Table 3. *Cont.*

Index	Author	Total of Citations	Title	Reference
6	Xie et al., 2019	630	A Survey of Blockchain Technology Applied to smart cities: Research Issues and Challenges	[252]
7	Zhang et al., 2017	620	Security and Privacy in smart city Applications: Challenges and Solutions	[370]
8	Sivanathan et al., 2019	579	Classifying IoT Devices in Smart Environments Using Network Traffic Characteristics	[371]
9	Sharma et al., 2017	500	Block-VN: A Distributed Blockchain-Based Vehicular Network Architecture in smart city	[372]
10	Khatoun et al., 2016	473	Smart cities: concepts, architectures, research opportunities	[373]
11	Djahel et al., 2015	436	A Communications-Oriented Perspective on Traffic Management Systems for Smart cities: Challenges and Innovative Approaches	[374]
12	Singh et al., 2020	429	Block IoT Intelligence: A Blockchain-enabled Intelligent IoT Architecture with Artificial Intelligence	[242]
13	Sharma et al., 2018	411	Blockchain-based hybrid network architecture for the smart city	[375]
14	Angelidou et al., 2017	390	The Role of smart city Characteristics in the Plans of Fifteen Cities	[376]
15	Rathore et al., 2018	330	Exploiting IoT and big data analytics: Defining Smart Digital City using real-time urban data	[377]
16	Memos et al., 2018	352	An Efficient Algorithm for Media-based Surveillance System (EAMSuS) in IoT smart city Framework	[188]
17	Aloqaily et al., 2019	353	An intrusion detection system for connected vehicles in smart cities	[56]
18	Braun et al., 2018	307	Security and privacy challenges in smart cities	[7]
19	Esposito et al., 2021	297	Blockchain-based authentication and authorization for smart city applications	[225]
20	Qiu et al., 2017	215	Heterogeneous ad hoc networks: Architectures, advances and challenges	[378]

These results show the importance and impact of smart city studies. Another important fact is that in recent years, new challenges regarding application information security in smart cities have emerged due to new technologies. As an output of the analytical process, papers have addressed these new issues and consequently have a high potential for being more cited in the future. For instance, the automation of vehicles in the field of intelligent transport systems [379] and human beings as potential targets for cyberattacks or even participating in a cyberattack with ethical implications for society.

4.3. Most Active and Cited Journals

Journals play an essential role in the development of a research area. Table 4 reports the most prominent journals in the number of publications on cybersecurity in the Scopus database and their impact factor in 2022.

Table 4. Journals and Impact Factors for information security and smart cities related literature.

Subject Areas	Source	Impact Factor 2022	# of Article
Computer Science	Computers and Security	5.6	262
	Future Generation Computer Systems	7.5	712
	IEEE Access	3.9	139
	IET Information Security	1.4	23
	Computer Communications	6	323
	IEEE Security and Privacy	1.9	54
	Computers in Human Behavior	9.9	60
	Information Technology and People	4.4	63
	International Journal of Communication Systems	2.1	256
	International Journal of Software Engineering and Knowledge Engineering	0.9	12
Social Sciences	Computer Law and Security Review	2.9	164
	Technological Forecasting and Social Change	12	346
	Public Administration Review	8.3	13
	Technology in Society	9.2	145
	Journal of Intellectual Capital	6	64
	Behavior and Information Technology	3.7	88
	International Journal of Human Computer Studies	5.4	27
	Business Horizons	7.4	58
	International Journal of Accounting Information Systems	4.6	12
Business, Management and Accounting	International Journal of Information Management	21	130
	Government Information Quarterly	7.8	157
	Information Technology for Development	4.261	47
	European Journal of Operational Research	6.363	33
	Information Sciences	8.1	131
Energy	Energies	3.2	195
	Sustainability	3.9	76
	Energy Research and Social Science	6.7	151
	Journal of Cleaner Production	11.1	465

It is worth mentioning that the top journals showing that the topic of information security and smart cities has attracted the attention of researchers from different fields. Because smart city is a multidisciplinary field, scholars often struggle to figure out the most appropriate outlet for their research that would have a significant impact. The information reported in this table indicates this willingness to publish in each specific area.

4.4. Country Co-Citation Analysis

In the next phase, the collaboration networks among countries were highlighted, as presented in Figure 4. The figure shows the distribution of countries with the most co-authorships. The clusters are indicated by circles and colors, explaining the proximity of the countries and the associations between co-authorships, while the edges illustrate how researchers' production is expanding. Notably, China (n = 462) presents the bigger production, followed by India (n = 411), the United States (n = 239), the United Kingdom (n = 146), Saudi Arabia (n = 125), South Korea (n = 102), Pakistan (n = 93), Australia (n = 71), Italy (n = 65), Spain (n = 63), Canada (n = 54), Taiwan (n = 51), Brazil (n = 49), Malaysia (n = 46), Turkey (n = 45), United Arab Emirate (n = 38), and Iran (n = 35).

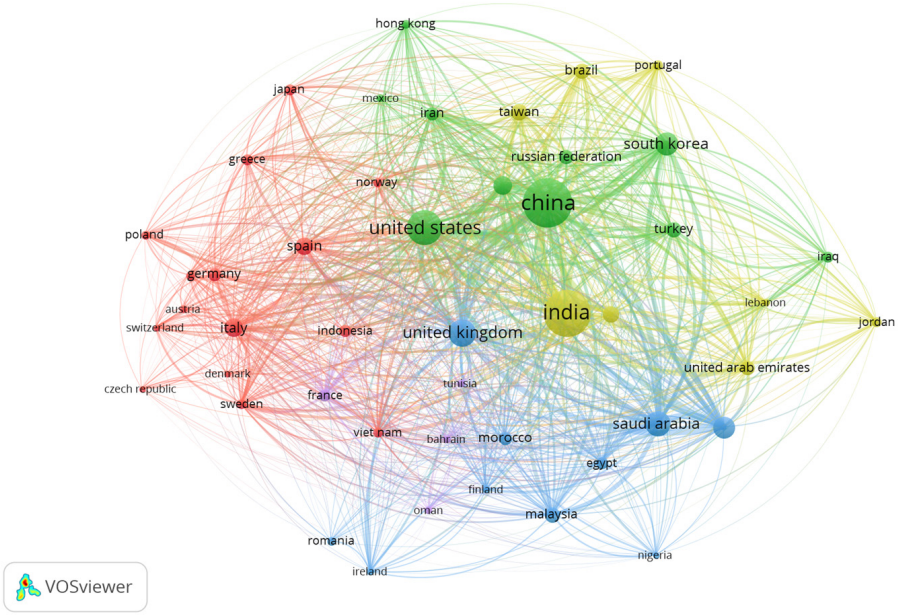

Figure 4. Collaboration networks on information security and smart cities among countries.

As can be seen, the research collaborations appear with a higher level of intensity among countries of the European Union and those of North America. In addition, there is also a collaboration network among Asia, North America, and Europe. Research collaboration in cybersecurity indicates the complexity of the interrelations and the opportunity for future cooperation. Also, the results allow three inferences to be drawn: countries with the most cooperation may offer practical implications for society through the partner with industries; academic experts affiliated with these countries can provide knowledge as references on the issue; and the contributions developed by the authors can serve as guidelines for other researches.

4.5. Keyword Co-Occurrence Analysis

Figure 5 highlights the network visualization for the most common terms used in the authors' keywords. The network reports the most relevant keywords of these items in terms of occurrences and their interactions between documents. A total of 267 keywords emerged, with at least one occurrence [380,381]. From this network, 36 items are considered independent, in which case the item does not bring any significant contribution to designing applicable queries and identifying pertinent empirical surveys. As expected, "Smart

city," "network security," and "security systems" stand out as the most common terms. However, upon closer examination of the other circles, correlations emerge concerning the topics presented in the paper. The blue cluster is associated with the analysis of surveillance and the application of methods for recognition. The green cluster is related to the analysis involving smart transportation. The purple cluster provides limited information about "cryptography" and contract management. The red cluster focuses on urban livability and its interaction with technology. The remaining terms do not exhibit significant expressiveness to readiness.

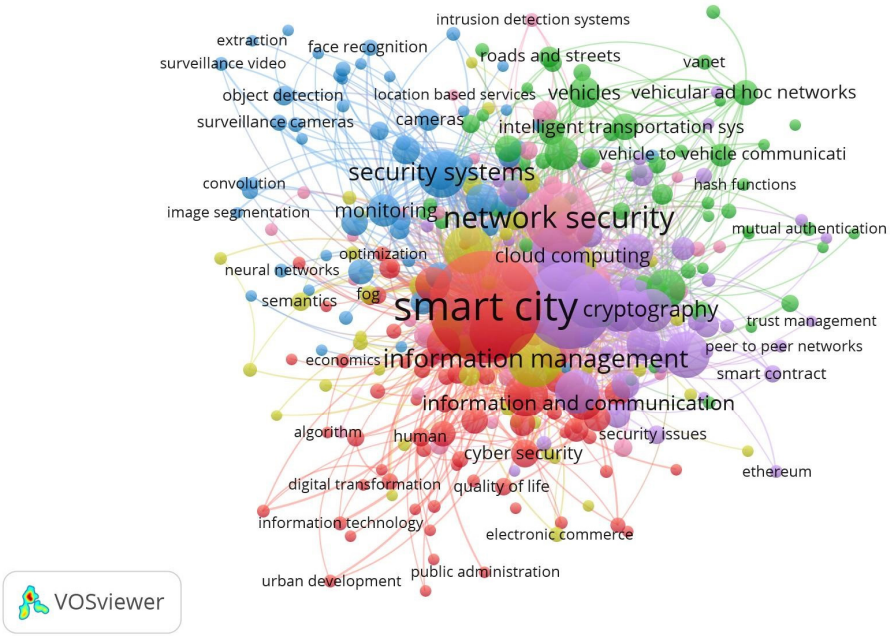

Figure 5. Most Relevant Keywords.

Table 5 details the keywords with the highest occurrences and interactions based on the set of complete articles published in journals indexed in Scopus, ranging from 2015 to 2023, as based on the network shown in Figure 5.

Table 5. High-frequency keywords for searches in the area between 2015 and 2023.

High-Frequency Keywords	Occurrences
Smart city	1146
Internet of Things	699
Network Security	470
Security	374
Computer Security	324
Cyber–Physical System	314
Data Information	291
Blockchain	198
Energy Efficiency	174
Energy Security	166
Cryptography	156
Green Computing	141
Information Security	139
Smart Grid	133
Sustainable Cities	131
Urban Development	127
Urban Planning	123
Accident Prevention, Attack Detection	119
Authentication, Authentication Protocols	117
Intelligent Transportation Systems, Information Exchanges	116

Table 5. *Cont.*

High-Frequency Keywords	Occurrences
Privacy Preservation	115
Public Key Cryptography	110
Network Protocols, Security Vulnerabilities	102

These results demonstrate that among the articles published, the keywords smart city and internet of things have the highest occurrence rates, which demonstrates the growing interest of researchers in topics related to information security and smart cities.

4.6. Methods in Cybersecurity

Methods play an essential role in the development of a research area. We have included Table 6 with 11 main cybersecurity methods applied in main areas such as Computer Science, Engineering, Mathematics, Social Sciences, Business Management, and Accounting.

Table 6. Cybersecurity methods and applications according to main areas.

Method	Computer Science	Engineering	Mathematics	Social Sciences	Business, Management and Accounting	Total
Risk Management	57	32	-	19	21	129
Machine Learning	48	17	7	9	11	101
Game Theory	28	17	9	8	2	64
Neural Network	17	15	4	-	5	41
Data Mining	25	5	2	-	5	37
Deep-Learning	18	7	3	1	2	33
Blockchain	17	8	3	2	3	33
Fuzzy Theory	16	6	5	-	2	29
Bayesian game	6	3	2	2	2	15
Software-Defined Networking	6	2	2	-	1	11
Natural Language Processing	4	2	-	-	1	7

These results demonstrate that Management Risk and Machine Learning have a total of 129 and 101 articles published, respectively. They allow the consideration of important factors that can lead to better decision-making in information security, and smart cities have become more widely used in actions focused on defense strategies.

5. Discussion

The discussion on information security and smart cities is not restricted to the area of computer science. The concern about data and information security is multidisciplinary and influences the evolution of different types of business. Health professionals, government institutions, academic environments, and several other stakeholders benefit from the opportunities for advancing research while they can take advantage of this study to indicate potential solutions and improve the level of information security, predicting the consequences of information loss [328,331]. For this, when planning on cybersecurity, it is necessary to prioritize strategic processes, actions, and tools that will be implemented or used, both for the organization, for the government/public administration, and for society in smart cities [376].

Smart cities use information and communication technologies to improve the quality of life of their inhabitants, making public services more efficient and creating innovative solutions to urban challenges [15]. However, as cities become more connected and dependent on technology systems, information security becomes an ever-increasing concern. Citizens' data, as well as operational information on critical city systems, can be at risk

from cyberattacks. Therefore, smart cities must have a comprehensive information security strategy to protect their systems and data [370]. This involves implementing cybersecurity measures at all layers of the city's infrastructure, from the communication network to IoT (Internet of Things) devices and data management systems [54,370].

To decrease the probability of a cyber threat causing damage, some cyber security measures should be implemented, such as Encryption, Authentication of users, Network Security, Cyber security training, and Regular software updates [90,382,383]. These shared vulnerabilities can be exploited by hackers and other malicious users to compromise city security, directly affecting citizens' lives. For example, a cyberattack on a traffic management system can lead to severe congestion and delays in emergency services. Some of the most common shared vulnerabilities in smart cities are weak passwords, delayed software updates, and unsafe IoT devices. This work contributes to presenting new information security technologies to minimize shared vulnerabilities in smart cities; it is essential to adopt comprehensive cybersecurity measures.

A challenge for developing countries will be the integration of smart cities. The decision to plan information security for the management of cities is essential to guarantee engagement in municipal services through intelligent digital systems. So, the smart city ecosystem requires new skills and competencies in various ways through strategic partnerships and contracts with service providers [373]. Maintaining a safe and smart city involves creating a public/private infrastructure to carry out activities and provide technologies that protect and protect citizens' information [286].

Four main considerations should be address regarding smart cities security:

1. Strategies for artificial intelligence and shared communications are necessary, ensuring opportune analysis of data/information flow through smart cities systems to detect threads and ensure the secure delivery of what must be communicated from one end to the other [22,384], and consequently providing the necessary confidentiality and privacy in communications [385];
2. Physical and cyber threats come from many areas, including state-sponsored critical infrastructure, criminals, natural disasters, and neglect of human agents [307,386,387], all opening several security holes that must be foreseen in risk containment plans to guarantee the integrity of the information that passes between the systems involved, demanding a smart cybersecurity architecture that can cover these risks [292];
3. Integrated operational management activities and knowledge sharing to prevent, mitigate, respond, and recover from incidents [388].
4. Acquiring emerging technologies that facilitate risk assessment ensures appropriate physical security and cybersecurity measures [172].

5.1. Addressing the Research Questions

The literature review developed had three research questions as its core, as presented in the methodological section. Based on literary findings, directions on these questions will now be presented.

RQ1—What are the patterns of information security applications found in research on smart cities?

This question can be addressed with the six clusters presented in Table 2, separating each cluster according to the main application domain areas, as follows:

(a) Smart Grids and Power Supply: this cluster covers works that mention applications that can cover information and cybersecurity on smart grids as a component of smart city systems to ensure efficient, safe, and sustainable power supply for citizens [226]. Smart grids cover topics such as bulk generation, transmission, distribution, customers, markets, service providers, and operations [78].

(b) Authentication as a security mechanism: this cluster covers applications regarding the control access policies and strategies for data protection in smart city systems, especially considering the large data volumes that are inherent to these systems [291].

Authentication mechanisms are projected to ensure privacy, trust, and reliability in the information and communication flows [51] to protect against invasion by attackers masquerading as legitimate users of the system [85].

(c) Cyberattack prevention/detection in smart cities: this cluster focuses on strategies to prevent or detect cyberattacks or vulnerabilities that may facilitate these attacks in the smart cities context, observing the best practices and methods to be applied in protecting involved systems [280]. The lack of these strategies can cause, for instance, theft of a user's sensitive data, utility fraud, and grid instability [1]. In other words, this can be considered a cluster containing works presenting core concepts and tools that are transversal to all other clusters.

(d) Security platforms for smart cities: this cluster involves not only technological platforms but the whole organizational and business instances needed to promote security to smart cities-related services and systems [60]. The main idea is to deliver quality of life for the users of these services and systems, which are any citizen in a smart city area [302]. Quick and efficient managerial decision-making is the main concept to ensure security platforms operate successfully in preventing risks from becoming events negatively affecting smart city services delivery for citizens [302]. These platforms are a means for aggregating concepts of the other five clusters, as can be understood by the diagram in Figure 6 in the answer for RQ2, synthesizing the relationships between all clusters of applications.

(e) Evaluation of threats to cybersecurity: this cluster deals with ways to evaluate threats to the smart cities systems, facilitating, for example, the design and management of security platforms and ensuring the necessary indicators and related analysis to promote the detection and prevention of cyberattacks [311,319]. It covers from devices to threat evaluation techniques, which can be used in support of security measures planning [6,54].

(f) Cybersecurity and society: this is the most comprehensive cluster, involving all the elements needed to promote cybersecurity for society, considering smart cities as cyber–physical systems [328]. It covers legal and ethical concepts, passing by managerial strategies and reaching the technical level with the frameworks of techniques/tools to ensure cybersecurity for people [333].

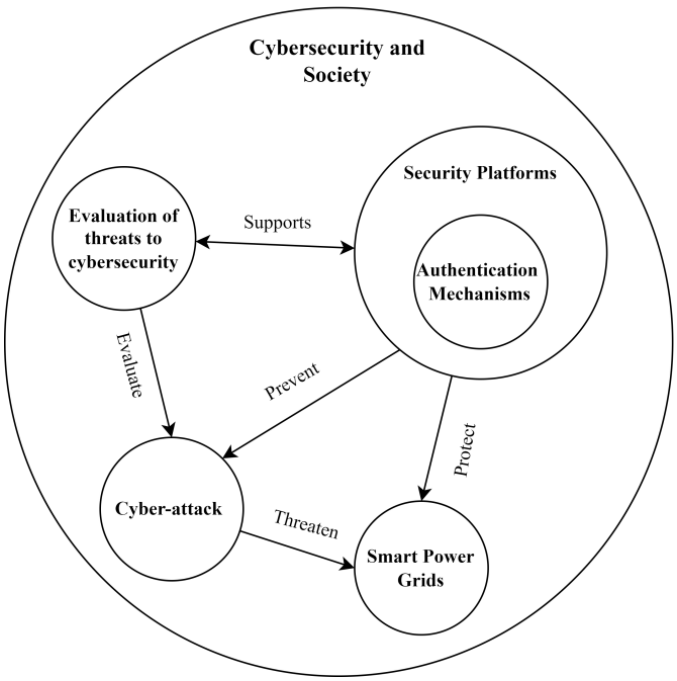

Figure 6. Relationships between the concepts involved in the applications clusters.

RQ2—What are the most demanding areas for information security in smart cities studies?

To answer this question, Figure 6 was created seeking to highlight the dynamics between the previously observed clusters. It should be noted that the diagram in the figure does not present a composition of works/authors found in the literature as in Figure 3, but the conceptual alignment and flow between the clusters.

Through this figure, we can see that the evaluation of threats to cybersecurity and security platforms are great "providers" within the set since several sectors within smart cities require constant monitoring and adequate analysis to detect threats, such as cyberattacks, and these assessments are fundamental to support the structuring and operationalization of security platforms. In turn, security platforms constitute essential components in smart cities to guarantee the dynamics of security in related systems, including smart grids, providing means for continuous evaluation of threats and preventing any kind of unauthorized access.

Another address that can be given to RQ2, as detected in the literature, is when it comes to the service provision sector. The most notable is energy supply, which gained prominence in a cluster that contained the largest number of jobs compared to the other clusters. However, other sectors receive several mentions in the literature, with the healthcare area being one of the most prominent. Table 3 indicates, for example, the work by Farahani et al. [155] in the line of IoT in medicine and healthcare as the one with the highest number of citations within the bibliographic base built for the bibliometric review. The third most cited work, by Rathore et al. [101], is also related to healthcare, proposing a framework based on blockchain for electronic health records. By the way, several of the works among the most cited are about the blockchain and related technologies appear in seven works (see [101,225,242,252,369,372,375]).

Blockchain, as a set of technologies for databases to ensure transparent data sharing, can be considered a core concept for the project of security platforms and systems in smart cities, being a transversal technical area that can be considered for smart grids and healthcare information security. Other areas, such as urban planning and building [54], transport/vehicles, and traffic control systems [56,372,374], can also be mentioned here as highlighted, as they are critical for the proper operation of smart cities, delivering quality of life and effective services to citizens.

RQ3—What research has the most influence on the application of information security and smart cities?

This question is also easily answered by the list of works in Table 3. It is intertwined with the comments made in the last two paragraphs of the previous section dedicated to RQ2. Following, the objectives of the top five most cited works are presented.

Farahani et al. [155], with 1001 citations, presented a survey of IoT Health and put forth a holistic eHealth ecosystem that encompasses various layers, including mobile health, assisted living, e-medicine, implants, early warning systems, and population monitoring.

Rathore et al. [54], with 996 citations, presented the proposal of a complete smart city architecture, also considering urban panning with data analysis on Big Data based on IoT.

Dagher et al. [101], with 746 citations, presented the proposal of a blockchain-powered framework designed to enable secure, seamless, and efficient access to medical records for patients, healthcare providers, and third parties while maintaining the privacy of sensitive patient information.

Biswas et al. [369], also with 746 citations, introduced a security framework that combines blockchain technology with smart devices, creating a secure communication platform within a smart city.

Elmaghraby et al. [15], with 640 citations, presented a survey on cybersecurity challenges, exploring two interconnected challenges, namely security and privacy. Additionally, they introduced a model for the interactions among individuals, servers, and IoT devices as the key elements in a smart city, emphasizing the necessity to safeguard these interactions.

5.2. Theoretical and Practical Implications

The results contribute to developing a practical perspective in computer science, particularly providing a conceptual framework integrated with information security and smart cities knowledge and leading research in the world. IT security professionals can take advantage of this study by using this structure as a reference to design new solutions in cybersecurity and formulate specific security policies to combat and prevent cyberattacks in smart cities. Moreover, this study shows the importance of developing information security strategies with a focus on user behavior in the city, characterized as the primary agent that causes security failures in IT solutions. In addition, IT researchers can obtain guidance to explore new fields of research, develop new trends and perspectives, develop applications to fill gaps in the literature and provide attention to different types of problems in information security and smart cities, which highlights the validity and relevance of this work.

Clustering bibliometric networks through co-citation analysis has practical contributions to the business area. By integrating knowledge between the disciplines of information and computing systems, managers and practitioners can quickly identify the most relevant concepts and best practices concerning information security and smart cities and perception of human behavior, smart power grid, online services, prevention systems for cyberattacks, the critical cyber infrastructures, threats, resilience, and social prospects of cybersecurity, designed by the clusters of co-citation analysis. As stated by [389], such a repository of terms associated with the scientific literature is a strategic tool for the continuous improvement of business, which can designate appropriate software features or necessary maintenance for the security of information systems and support decision methods in the treatment and prevention of information security incidents. This systematic view can also highlight organizations' responsibility of managers for smart city decisions related to control and data privacy and potential correlations between data security and the organization's value judgments on security devices.

Although developments and research related to the creation of control software, infrastructure improvement, risk prevention, and failure prevention, investment in IoT and Data solutions Science have increased in the last ten years, as shown by the results of this research, cybersecurity is still treated as a secondary element in government organizations and institutions in developing countries. In this context, the acquisition of new IT solutions must be considered a strategy as important as the investment in cybersecurity, as it can directly affect the users' perception of smart cities. Service providers must adhere to service-level agreements regarding system operation, data generation, and the use and sharing of information. Additionally, they should undergo privacy impact assessments to ensure compliance with privacy regulations and protect individuals' personal information. By enforcing these requirements, organizations can ensure that service providers maintain a high standard of service delivery, respect privacy rights, and safeguard sensitive data.

This research presents an integrative theoretical framework conceptualized in the presentation of the state of the art on the scope of application and development of the term "information security and smart cities." The theoretical framework presented can provide conceptual support to researchers and professionals in the field and can be used as a reference for understanding the connections between the lines of research, the composition of clusters of researchers, and the relationship between related areas, and can serve as a conceptual basis for the cybersecurity planning project in different businesses.

6. Conclusions

This study reported the construction of a systematic review involving bibliometric aspects, oriented to the identification of the main applications of the information security and smart cities concept, such as cybersecurity and human perception behavior, cybersecurity and smart electrical network, cybersecurity control and data in services online and intrusion detection for cybersecurity. The analysis, spanning articles from 2015 to 2023 in Scopus-indexed journals, leveraged VOSviewer software for mapping global researchers and their

contributions. The findings underscored the interdisciplinary nature of information security and smart cities, emphasizing their relevance beyond computational sciences.

The study's outcomes offer valuable insights for managers, professionals, and academics across diverse domains, highlighting opportunities for exploration within the literature of cybersecurity in smart cities. The implications of information security and smart cities extend beyond computational sciences, influencing business actions, social development, and service enhancement. The results emphasize the need for interdisciplinary approaches in cybersecurity research, indicating collaboration across engineering, administration, psychology, economics, and law. Furthermore, the study advocates for a holistic perspective in cybersecurity research, promoting interdisciplinarity and encompassing ethical considerations for effective business strategies in the digital era.

Noteworthy findings include the identification of leading countries in cybersecurity studies, with China, India, the United States, and the United Kingdom taking the forefront. The study observes a lack of exploration in cybersecurity studies in developing nations, often attributed to technological limitations. It also notes a growing trend of international collaboration among researchers in the field. There is a need for research in cybersecurity solutions, particularly in the context of virtual service systems such as telehealth services within smart cities.

Although the work has a full scope in information security and smart cities, some limitations can be mentioned, such as potential oversight of frontier applications during the detailed analysis and the lack of considerations for cybersecurity software in this review. This could be an exciting gap for future research, including a comprehensive assessment of cybersecurity software options similar to the work of Daraio et al. [389] on efficiency frontier applications.

There is a growing call for collective initiatives and educational campaigns centered on information security. A deeper public understanding in this domain can catalyze a stronger trust in the technologies underpinning smart cities, bolstering their adoption and seamless integration into citizens' daily lives. Information security is undeniably a foundational pillar for the successful assimilation of these technologies. Consequently, it becomes imperative to address not only the technical facets but also the subjective and objective dimensions highlighted in this study, which impact the global landscape.

Author Contributions: Conceptualization, T.P. and T.C.C.N.; methodology, T.P., L.C.B.d.O.F., R.C.P.d.O. and T.C.C.N.; software, T.P.; validation, V.D.H.d.C., T.C.C.N. and C.J.J.F.; formal analysis, T.P. and L.C.B.d.O.F.; investigation, T.P., R.C.P.d.O., T.C.C.N. and V.D.H.d.C.; resources, T.P.; data curation, T.P.; writing—original draft preparation, T.P. and V.D.H.d.C.; writing—review and editing, V.D.H.d.C. and C.J.J.F.; visualization, T.P.; supervision, T.C.C.N. and V.D.H.d.C.; project administration, T.P.; funding acquisition, T.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data presented in this study is only contained in the article itself.

Acknowledgments: We want to acknowledge the support from the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES, Brazil), the Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq, Brazil), the Universidade Federal do Pará (UFPA, Brazil), the Universidade Federal de Alagoas (UFAL, Brazil), the Universidade Federal de Pernambuco (UFPE, Brazil), and the Universidade Federal Rural do Semi-Árido (UFERSA, Brazil).

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

References

1. Alfouzan, F.A.; Kim, K.; Alzahrani, N.M. An Efficient Framework for Securing the Smart City Communication Networks. *Sensors* **2022**, *22*, 3053. [CrossRef]
2. Belgaum, M.R.; Alansari, Z.; Jain, R.; Alshaer, J. A Framework for Evaluation of Cyber Security Challenges in Smart Cities. In Proceedings of the Smart Cities Symposium, Zallaq, Bahrain, 22–23 April 2018; Institution of Engineering and Technology: London, UK, 2018; p. 295.

3. Sharma, G.; Kalra, S. A Secure Remote User Authentication Scheme for Smart Cities E-Governance Applications. *J. Reliab. Intell. Environ.* **2017**, *3*, 177–188. [CrossRef]
4. Naqvi, N.; Ur Rehman, S.; Islam, Z. A Hyperconnected Smart City Framework. *Australas. J. Inf. Syst.* **2020**, *24*. Available online: https://journal.acs.org.au/index.php/ajis/article/view/2531 (accessed on 17 October 2023). [CrossRef]
5. Arasteh, H.; Hosseinnezhad, V.; Loia, V.; Tommasetti, A.; Troisi, O.; Shafie-khah, M.; Siano, P. Iot-Based Smart Cities: A Survey. In Proceedings of the 2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC), Florence, Italy, 7–10 June 2016; IEEE: New York, NY, USA, 2016; pp. 1–6.
6. Mohamed, N.; Al-Jaroodi, J.; Jawhar, I.; Idries, A.; Mohammed, F. Unmanned Aerial Vehicles Applications in Future Smart Cities. *Technol. Forecast. Soc. Change* **2020**, *153*, 119293. [CrossRef]
7. Braun, T.; Fung, B.C.M.; Iqbal, F.; Shah, B. Security and Privacy Challenges in Smart Cities. *Sustain. Cities Soc.* **2018**, *39*, 499–507. [CrossRef]
8. Gourisetti, S.N.G.; Mylrea, M.; Patangia, H. Cybersecurity Vulnerability Mitigation Framework through Empirical Paradigm: Enhanced Prioritized Gap Analysis. *Futur. Gener. Comput. Syst.* **2020**, *105*, 410–431. [CrossRef]
9. Nieto, A.; Acien, A.; Fernandez, G. Crowdsourcing Analysis in 5G IoT: Cybersecurity Threats and Mitigation. *Mob. Netw. Appl.* **2019**, *24*, 881–889. [CrossRef]
10. Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M. Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. *Futur. Gener. Comput. Syst.* **2013**, *29*, 1645–1660. [CrossRef]
11. Ma, C. Smart City and Cyber-Security; Technologies Used, Leading Challenges and Future Recommendations. *Energy Rep.* **2021**, *7*, 7999–8012. [CrossRef]
12. Habib, M.Y.; Qureshi, H.A.; Khan, S.A.; Mansoor, Z.; Chishti, A.R. Cybersecurity and Smart Cities: Current Status and Future. In Proceedings of the 2023 IEEE International Conference on Emerging Trends in Engineering, Sciences and Technology (ICES&T), Bahawalpur, Pakistan, 9–11 January 2023; IEEE: New York, NY, USA, 2023; pp. 1–7.
13. Behnam, A.; Azad, S.; Daneshvar, M.; Anvari-Moghaddam, A.; Marzband, M. Artificial Intelligence–Enabled Internet of Things Technologies in Modern Energy Grids. In *IoT Enabled Multi-Energy Systems*; Elsevier: Amsterdam, The Netherlands, 2023; pp. 69–86.
14. Kim, K.; Alshenaifi, I.M.; Ramachandran, S.; Kim, J.; Zia, T.; Almorjan, A. Cybersecurity and Cyber Forensics for Smart Cities: A Comprehensive Literature Review and Survey. *Sensors* **2023**, *23*, 3681. [CrossRef]
15. Elmaghraby, A.S.; Losavio, M.M. Cyber Security Challenges in Smart Cities: Safety, Security and Privacy. *J. Adv. Res.* **2014**, *5*, 491–497. [CrossRef] [PubMed]
16. Xia, L.; Semirumi, D.T.; Rezaei, R. A Thorough Examination of Smart City Applications: Exploring Challenges and Solutions throughout the Life Cycle with Emphasis on Safeguarding Citizen Privacy. *Sustain. Cities Soc.* **2023**, *98*, 104771. [CrossRef]
17. Anisetti, M.; Ardagna, C.; Bellandi, V.; Cremonini, M.; Frati, F.; Damiani, E. Privacy-Aware Big Data Analytics as a Service for Public Health Policies in Smart Cities. *Sustain. Cities Soc.* **2018**, *39*, 68–77. [CrossRef]
18. Baig, Z.A.; Szewczyk, P.; Valli, C.; Rabadia, P.; Hannay, P.; Chernyshev, M.; Johnstone, M.; Kerai, P.; Ibrahim, A.; Sansurooah, K.; et al. Future Challenges for Smart Cities: Cyber-Security and Digital Forensics. *Digit. Investig.* **2017**, *22*, 3–13. [CrossRef]
19. Caragliu, A.; Del Bo, C.F. Smart Innovative Cities: The Impact of Smart City Policies on Urban Innovation. *Technol. Forecast. Soc. Change* **2019**, *142*, 373–383. [CrossRef]
20. Kitchin, R.; Dodge, M. The (In)Security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention. *J. Urban Technol.* **2019**, *26*, 47–65. [CrossRef]
21. Sharma, K.; Mukhopadhyay, A. Sarima-Based Cyber-Risk Assessment and Mitigation Model for A Smart City's Traffic Management Systems (Scram). *J. Organ. Comput. Electron. Commer.* **2022**, *32*, 1–20. [CrossRef]
22. Rao, P.M.; Deebak, B.D. Security and Privacy Issues in Smart Cities/Industries: Technologies, Applications, and Challenges. *J. Ambient Intell. Humaniz. Comput.* **2023**, *14*, 10517–10553. [CrossRef]
23. Lai, C.S.; Jia, Y.; Dong, Z.; Wang, D.; Tao, Y.; Lai, Q.H.; Wong, R.T.K.; Zobaa, A.F.; Wu, R.; Lai, L.L. A Review of Technical Standards for Smart Cities. *Clean Technol.* **2020**, *2*, 290–310. [CrossRef]
24. Yigitcanlar, T.; Kankanamge, N.; Vella, K. How Are Smart City Concepts and Technologies Perceived and Utilized? A Systematic Geo-Twitter Analysis of Smart Cities in Australia. *J. Urban Technol.* **2021**, *28*, 135–154. [CrossRef]
25. Verhulsdonck, G.; Weible, J.L.; Helser, S.; Hajduk, N. Smart Cities, Playable Cities, and Cybersecurity: A Systematic Review. *Int. J. Hum. Comput. Interact.* **2023**, *39*, 378–390. [CrossRef]
26. Boni, A.; López-Fogués, A.; Fernández-Baldor, Á.; Millan, G.; Belda-Miquel, S. Initiatives towards a Participatory Smart City. The Role of Digital Grassroots Innovations. *J. Glob. Ethics* **2019**, *15*, 168–182. [CrossRef]
27. Xu, N.; Ding, Y.; Guo, J. Do Smart City Policies Make Cities More Innovative: Evidence from China. *J. Asian Public Policy* **2022**, *15*, 1–17. [CrossRef]
28. Habib, A.; Alsmadi, D.; Prybutok, V.R. Factors That Determine Residents' Acceptance of Smart City Technologies. *Behav. Inf. Technol.* **2020**, *39*, 610–623. [CrossRef]
29. Langer, L.; Skopik, F.; Smith, P.; Kammerstetter, M. From Old to New: Assessing Cybersecurity Risks for an Evolving Smart Grid. *Comput. Secur.* **2016**, *62*, 165–176. [CrossRef]
30. Silva, M.M.; Costa, A.P.C.S.; de Gusmão, A.P.H. Continuous Cooperation: A Proposal Using a Fuzzy Multicriteria Sorting Method. *Int. J. Prod. Econ.* **2014**, *151*, 67–75. [CrossRef]

31. De Gusmão, A.P.H.; Silva, L.C.E.; Silva, M.M.; Poleto, T.; Costa, A.P.C.S. Information Security Risk Analysis Model Using Fuzzy Decision Theory. *Int. J. Inf. Manag.* **2016**, *36*, 25–34. [CrossRef]
32. Poleto, T.; Silva, M.M.; Clemente, T.R.N.; de Gusmão, A.P.H.; Araújo, A.P.D.B.; Costa, A.P.C.S. A Risk Assessment Framework Proposal Based on Bow-Tie Analysis for Medical Image Diagnosis Sharing within Telemedicine. *Sensors* **2021**, *21*, 2426. [CrossRef]
33. Rodgers, W.; Alhendi, E.; Xie, F. The Impact of Foreignness on the Compliance with Cybersecurity Controls. *J. World Bus.* **2019**, *54*, 101012. [CrossRef]
34. De Gusmão, A.P.H.; Silva, M.M.; Poleto, T.; Silva, L.C.; Costa, A.P.C.S. Cybersecurity Risk Analysis Model Using Fault Tree Analysis and Fuzzy Decision Theory. *Int. J. Inf. Manag.* **2018**, *43*, 248–260. [CrossRef]
35. Makhdoom, I.; Abolhasan, M.; Lipman, J.; Liu, R.P.; Ni, W. Anatomy of Threats to the Internet of Things. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 1636–1675. [CrossRef]
36. Kruse, C.S.; Frederick, B.; Jacobson, T.; Monticone, D.K. Cybersecurity in Healthcare: A Systematic Review of Modern Threats and Trends. *Technol. Health Care* **2017**, *25*, 1–10. [CrossRef] [PubMed]
37. Stamatellis, C.; Papadopoulos, P.; Pitropakis, N.; Katsikas, S.; Buchanan, W.J. A Privacy-Preserving Healthcare Framework Using Hyperledger Fabric. *Sensors* **2020**, *20*, 6587. [CrossRef]
38. Cabaj, K.; Domingos, D.; Kotulski, Z.; Respício, A. Cybersecurity Education: Evolution of the Discipline and Analysis of Master Programs. *Comput. Secur.* **2018**, *75*, 24–35. [CrossRef]
39. Li, X.; Shan, Z.; Liu, F.; Chen, Y.; Hou, Y. A Consistently-Executing Graph-Based Approach for Malware Packer Identification. *IEEE Access* **2019**, *7*, 51620–51629. [CrossRef]
40. Habibzadeh, H.; Nussbaum, B.H.; Anjomshoa, F.; Kantarci, B.; Soyata, T. A Survey on Cybersecurity, Data Privacy, and Policy Issues in Cyber-Physical System Deployments in Smart Cities. *Sustain. Cities Soc.* **2019**, *50*, 101660. [CrossRef]
41. Shin, S.; Lee, S.; Burian, S.J.; Judi, D.R.; McPherson, T. Evaluating Resilience of Water Distribution Networks to Operational Failures from Cyber-Physical Attacks. *J. Environ. Eng.* **2020**, *146*, 04020003. [CrossRef]
42. Collier, Z.A.; Dimase, D.; Walters, S.; Tehranipoor, M.M.; Lambert, J.H.; Linkov, I. Cybersecurity Standards: Managing Risk and Creating Resilience. *Computer* **2014**, *47*, 70–76. [CrossRef]
43. Cybersecurity, Critical Infrastructure. Framework for Improving Critical Infrastructure Cybersecurity. *Proc. Annu. ISA Anal. Div. Symp.* **2018**, *535*, 9–25.
44. Ben-Asher, N.; Gonzalez, C. Effects of Cyber Security Knowledge on Attack Detection. *Comput. Hum. Behav.* **2015**, *48*, 51–61. [CrossRef]
45. Boyson, S. Cyber Supply Chain Risk Management: Revolutionizing the Strategic Control of Critical IT Systems. *Technovation* **2014**, *34*, 342–353. [CrossRef]
46. Kawaguchi, H.; Tone, K.; Tsutsui, M. Estimation of the Efficiency of Japanese Hospitals Using a Dynamic and Network Data Envelopment Analysis Model. *Health Care Manag. Sci.* **2014**, *17*, 101–112. [CrossRef]
47. Kim, Y.S.; Tague, P.; Lee, H.; Kim, H. A Jamming Approach to Enhance Enterprise Wi-Fi Secrecy through Spatial Access Control. *Wirel. Netw.* **2015**, *21*, 2631–2647. [CrossRef]
48. Kritzinger, E.; Von Solms, S.H. Cyber Security for Home Users: A New Way of Protection through Awareness Enforcement. *Comput. Secur.* **2010**, *29*, 840–847. [CrossRef]
49. Pfleeger, S.L.; Caputo, D.D. Leveraging Behavioral Science to Mitigate Cyber Security Risk. *Comput. Secur.* **2012**, *31*, 597–611. [CrossRef]
50. Razzaq, A.; Sharif, A.; Ozturk, I.; Skare, M. Asymmetric Influence of Digital Finance, and Renewable Energy Technology Innovation on Green Growth in China. *Renew. Energy* **2023**, *202*, 310–319. [CrossRef]
51. Asif, M.; Aziz, Z.; Bin Ahmad, M.; Khalid, A.; Waris, H.A.; Gilani, A. Blockchain-Based Authentication and Trust Management Mechanism for Smart Cities. *Sensors* **2022**, *22*, 2604. [CrossRef] [PubMed]
52. Anomah, S.; Ayeboafo, B.; Aguabeng, O. A Conceptual Model for Comprehensive Assurance Review Engagements for Less Developed Regulatory Environments. *EDPACS* **2023**, *67*, 1–29. [CrossRef]
53. Nandan, M.; Singh, A.; Mandayam, G. Social Value Creation and Social Innovation by Human Service Professionals: Evidence from Missouri, USA. *Adm. Sci.* **2019**, *9*, 86. [CrossRef]
54. Rathore, M.M.; Ahmad, A.; Paul, A.; Rho, S. Urban Planning and Building Smart Cities Based on the Internet of Things Using Big Data Analytics. *Comput. Netw.* **2016**, *101*, 63–80. [CrossRef]
55. Pohls, H.C.; Angelakis, V.; Suppan, S.; Fischer, K.; Oikonomou, G.; Tragos, E.Z.; Rodriguez, R.D.; Mouroutis, T. RERUM: Building a Reliable IoT upon Privacy- and Security- Enabled Smart Objects. In Proceedings of the 2014 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), Istanbul, Turkey, 6–9 April 2014; IEEE: New York, NY, USA, 2014; pp. 122–127.
56. Aloqaily, M.; Otoum, S.; Al Ridhawi, I.; Jararweh, Y. An Intrusion Detection System for Connected Vehicles in Smart Cities. *Ad Hoc Netw.* **2019**, *90*, 101842. [CrossRef]
57. Chen, H.C.; You, I.; Weng, C.E.; Cheng, C.H.; Huang, Y.F. A Security Gateway Application for End-to-End M2M Communications. *Comput. Stand. Interfaces* **2016**, *44*, 85–93. [CrossRef]
58. Cowley, J.A.; Greitzer, F.L.; Woods, B. Effect of Network Infrastructure Factors on Information System Risk Judgments. *Comput. Secur.* **2015**, *52*, 142–158. [CrossRef]
59. Asri, S.; Pranggono, B. Impact of Distributed Denial-of-Service Attack on Advanced Metering Infrastructure. *Wirel. Pers. Commun.* **2015**, *83*, 2211–2223. [CrossRef]

60. Ismagilova, E.; Hughes, L.; Rana, N.P.; Dwivedi, Y.K. Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework. *Inf. Syst. Front.* **2022**, *24*, 393–414. [CrossRef]
61. Zhou, J. Artificial Intelligence-Based Recommendation and Application of Public Services in Smart Cities. *Comput. Intell. Neurosci.* **2022**, *2022*, 8958865. [CrossRef]
62. Mora, L.; Gerli, P.; Ardito, L.; Messeni Petruzzelli, A. Smart City Governance from an Innovation Management Perspective: Theoretical Framing, Review of Current Practices, and Future Research Agenda. *Technovation* **2023**, *123*, 102717. [CrossRef]
63. Azzaoui, A.; El Singh, S.K.; Pan, Y.; Park, J.H. Block5GIntell: Blockchain for AI-Enabled 5G Networks. *IEEE Access* **2020**, *8*, 145918–145935. [CrossRef]
64. He, Y.; Zhang, M.; Yang, X.; Luo, J.; Chen, Y. A Survey of Privacy Protection and Network Security in User On-Demand Anonymous Communication. *IEEE Access* **2020**, *8*, 54856–54871. [CrossRef]
65. Lin, H.; Chen, C.; Wang, J.; Qi, J.; Jin, D.; Kalbarczyk, Z.T.; Iyer, R.K. Self-Healing Attack-Resilient PMU Network for Power System Operation. *IEEE Trans. Smart Grid* **2018**, *9*, 1551–1565. [CrossRef]
66. Shin, J.; Son, H.; Khalil ur, R.; Heo, G. Development of a Cyber Security Risk Model Using Bayesian Networks. *Reliab. Eng. Syst. Saf.* **2015**, *134*, 208–217. [CrossRef]
67. Verma, V.K.; Singh, S.; Pathak, N.P. Impact of Malicious Servers over Trust and Reputation Models in Wireless Sensor Networks. *Int. J. Electron.* **2016**, *103*, 530–540. [CrossRef]
68. Gartner Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly $600 Billion in 2023. Available online: http://www.gartner.com/en/industries/high-tech. (accessed on 17 October 2023).
69. Luo, Y.; Xu, M.; Huang, K.; Wang, D.; Fu, S. Efficient Auditing for Shared Data in the Cloud with Secure User Revocation and Computations Outsourcing. *Comput. Secur.* **2018**, *73*, 492–506. [CrossRef]
70. Butpheng, C.; Yeh, K.-H.; Xiong, H. Security and Privacy in IoT-Cloud-Based e-Health Systems—A Comprehensive Review. *Symmetry* **2020**, *12*, 1191. [CrossRef]
71. Dinh, T.; Kim, Y. A Novel Location-Centric IoT-Cloud Based On-Street Car Parking Violation Management System in Smart Cities. *Sensors* **2016**, *16*, 810. [CrossRef]
72. Marwan, M.; Kartit, A.; Ouahmane, H. Security Enhancement in Healthcare Cloud Using Machine Learning. *Procedia Comput. Sci.* **2018**, *127*, 388–397. [CrossRef]
73. NIST Big Data Public Working Group. *Big Data Interoperability Framework: Security and Privacy*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2015; Volume 4, p. 75.
74. Bojanc, R.; Jerman-Blažič, B.; Tekavčič, M. Managing the Investment in Information Security Technology by Use of a Quantitative Modeling. *Inf. Process. Manag.* **2012**, *48*, 1031–1052. [CrossRef]
75. Tweneboah-Koduah, S.; Skouby, K.E.; Tadayoni, R. Cyber Security Threats to IoT Applications and Service Domains. *Wirel. Pers. Commun.* **2017**, *95*, 169–185. [CrossRef]
76. Aceto, G.; Persico, V.; Pescapé, A. The Role of Information and Communication Technologies in Healthcare: Taxonomies, Perspectives, and Challenges. *J. Netw. Comput. Appl.* **2018**, *107*, 125–154. [CrossRef]
77. Whitley, E.A. Informational Privacy, Consent and the "Control" of Personal Data. *Inf. Secur. Tech. Rep.* **2009**, *14*, 154–159. [CrossRef]
78. Wang, W.; Lu, Z. Cyber Security in the Smart Grid: Survey and Challenges. *Comput. Netw.* **2013**, *57*, 1344–1371. [CrossRef]
79. El-Gayar, O.F.; Fritz, B.D. A Web-Based Multi-Perspective Decision Support System for Information Security Planning. *Decis. Support Syst.* **2010**, *50*, 43–54. [CrossRef]
80. Chen, R.-M.; Hsieh, K.-T. Effective Allied Network Security System Based on Designed Scheme with Conditional Legitimate Probability against Distributed Network Attacks and Intrusions. *Int. J. Commun. Syst.* **2012**, *25*, 672–688. [CrossRef]
81. Varadharajan, V.; Tupakula, U. Counteracting Security Attacks in Virtual Machines in the Cloud Using Property Based Attestation. *J. Netw. Comput. Appl.* **2014**, *40*, 31–45. [CrossRef]
82. Jolly, P.K.; Batra, S. Security against Attacks and Malicious Code Execution in Mobile Agent Using IBF-CPABE Protocol. *Wirel. Pers. Commun.* **2019**, *107*, 1155–1169. [CrossRef]
83. Chuang, Y.-H.; Lei, C.-L.; Shiu, H.-J. How to Design a Secure Anonymous Authentication and Key Agreement Protocol for Multi-Server Environments and Prove Its Security. *Symmetry* **2021**, *13*, 1629. [CrossRef]
84. Bojanc, R.; Jerman-Blažič, B. Standard Approach for Quantification of the ICT Security Investment for Cybercrime Prevention. In Proceedings of the 2008 Second International Conference on the Digital Society (ICDS), Saint Luce, Martinique, 10–15 February 2008; IEEE: New York, NY, USA; Volume 30, pp. 7–14. [CrossRef]
85. Saber, O.; Mazri, T. Smart City Security Issues: The Main Attacks and Countermeasures. *Int. Arch. Photogramm. Remote Sens. Spat. Inf. Sci.* **2021**, *46*, 465–472. [CrossRef]
86. Andriole, K.P. Security of Electronic Medical Information and Patient Privacy: What You Need to Know. *J. Am. Coll. Radiol.* **2014**, *11*, 1212–1216. [CrossRef]
87. Ullah, F.; Ali Babar, M. Architectural Tactics for Big Data Cybersecurity Analytics Systems: A Review. *J. Syst. Softw.* **2019**, *151*, 81–118. [CrossRef]
88. Kshetri, N. Blockchain's Roles in Strengthening Cybersecurity and Protecting Privacy. *Telecomm. Policy* **2017**, *41*, 1027–1038. [CrossRef]

89. Daoudagh, S.; Marchetti, E.; Savarino, V.; Bernabe, J.B.; García-Rodríguez, J.; Moreno, R.T.; Martinez, J.A.; Skarmeta, A.F. Data Protection by Design in the Context of Smart Cities: A Consent and Access Control Proposal. *Sensors* **2021**, *21*, 7154. [CrossRef]
90. Zhou, L.; Thieret, R.; Watzlaf, V.; Dealmeida, D.; Parmanto, B. A Telehealth Privacy and Security Self-Assessment Questionnaire for Telehealth Providers: Development and Validation. *Int. J. Telerehabil.* **2019**, *11*, 3–14. [CrossRef] [PubMed]
91. Rehman, A.; Haseeb, K.; Saba, T.; Lloret, J.; Ahmed, Z. Mobility Support 5G Architecture with Real-Time Routing for Sustainable Smart Cities. *Sustainability* **2021**, *13*, 9092. [CrossRef]
92. Nabi, F. Designing a Framework Method for Secure Business Application Logic Integrity in E-Commerce Systems. *Int. J. Netw. Secur.* **2011**, *12*, 29–41. [CrossRef]
93. Ikrissi, G.; Mazri, T. Iot-Based Smart Environments: State of the Art, Security Threats and Solutions. *Int. Arch. Photogramm. Remote Sens. Spat. Inf. Sci.* **2021**, *46*, 279–286. [CrossRef]
94. Awan, K.A.; Ud Din, I.; Almogren, A.; Almajed, H. AgriTrust—A Trust Management Approach for Smart Agriculture in Cloud-Based Internet of Agriculture Things. *Sensors* **2020**, *20*, 6174. [CrossRef]
95. Raoof, A.; Matrawy, A. The Effect of Buffer Management Strategies on 6LoWPAN's Response to Buffer Reservation Attacks. In Proceedings of the IEEE International Conference on Communications, Paris, France, 21–25 May 2017; pp. 1–7. [CrossRef]
96. Sohal, A.S.; Sandhu, R.; Sood, S.K.; Chang, V. A Cybersecurity Framework to Identify Malicious Edge Device in Fog Computing and Cloud-of-Things Environments. *Comput. Secur.* **2018**, *74*, 340–354. [CrossRef]
97. Sasaki, T.; Morita, Y.; Jada, A. Access Control Architecture for Smart City IoT Platform. In Proceedings of the 2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), Rotorua, New Zealand, 5–8 August 2018; IEEE: New York, NY, USA, 2019; pp. 717–722.
98. Wang, F.; Luo, W. Assessing Spatial and Nonspatial Factors for Healthcare Access: Towards an Integrated Approach to Defining Health Professional Shortage Areas. *Health Place* **2005**, *11*, 131–146. [CrossRef]
99. Banerjee, S.; Roy, S.; Odelu, V.; Das, A.K.; Chattopadhyay, S.; Rodrigues, J.J.P.C.; Park, Y. Multi-Authority CP-ABE-Based User Access Control Scheme with Constant-Size Key and Ciphertext for IoT Deployment. *J. Inf. Secur. Appl.* **2020**, *53*, 102503. [CrossRef]
100. Di Francesco Maesa, D.; Mori, P.; Ricci, L. A Blockchain Based Approach for the Definition of Auditable Access Control Systems. *Comput. Secur.* **2019**, *84*, 93–119. [CrossRef]
101. Dagher, G.G.; Mohler, J.; Milojkovic, M.; Marella, P.B. Ancile: Privacy-Preserving Framework for Access Control and Interoperability of Electronic Health Records Using Blockchain Technology. *Sustain. Cities Soc.* **2018**, *39*, 283–297. [CrossRef]
102. Ferreira, D.C.; Marques, R.C. Do Quality and Access to Hospital Services Impact on Their Technical Efficiency? *Omega* **2019**, *86*, 218–236. [CrossRef]
103. Kang, M.; Robards, F.; Luscombe, G.; Sanci, L.A.; Hawke, C.I.; Steinbeck, K.S.; Jan, S.; Kong, M.J.; Usherwood, T.P. Understanding Access and Equity: Associations between Barriers to Health Care and Social Marginalisation. *J. Adolesc. Heal.* **2018**, *62*, S28–S29. [CrossRef]
104. Shi, M.; Jiang, R.; Hu, X.; Shang, J. A Privacy Protection Method for Health Care Big Data Management Based on Risk Access Control. *Health Care Manag. Sci.* **2019**, *23*, 427–442. [CrossRef] [PubMed]
105. Hsu, C.; Zeng, B.; Zhang, M. A Novel Group Key Transfer for Big Data Security Q. *Appl. Math. Comput.* **2014**, *249*, 436–443. [CrossRef]
106. Moreno-Sanchez, R.; Hayden, M.; Janes, C.; Anderson, G. A Web-Based Multimedia Spatial Information System to Document Aedes Aegypti Breeding Sites and Dengue Fever Risk along the US-Mexico Border. *Heal. Place* **2006**, *12*, 715–727. [CrossRef]
107. Mendonça Silva, M.; Poleto, T.; Silva, L.C.E.; Henriques De Gusmao, A.P.; Cabral Seixas Costa, A.P. A Grey Theory Based Approach to Big Data Risk Management Using FMEA. *Math. Probl. Eng.* **2016**, *2016*, 9175418. [CrossRef]
108. Wang, J.; Paschalidis, I.C. Botnet Detection Based on Anomaly and Community Detection. *IEEE Trans. Control Netw. Syst.* **2017**, *4*, 392–404. [CrossRef]
109. Singh, K.; Guntuku, S.C.; Thakur, A.; Hota, C. Big Data Analytics Framework for Peer-to-Peer Botnet Detection Using Random Forests. *Inf. Sci.* **2014**, *278*, 488–497. [CrossRef]
110. Kim, D.W.; Yan, P.; Zhang, J. Detecting Fake Anti-Virus Software Distribution Webpages. *Comput. Secur.* **2015**, *49*, 95–106. [CrossRef]
111. Alotaibi, S.S. Registration Center Based User Authentication Scheme for Smart E-Governance Applications in Smart Cities. *IEEE Access* **2019**, *7*, 5819–5833. [CrossRef]
112. Deypir, M.; Horri, A. Instance Based Security Risk Value Estimation for Android Applications. *J. Inf. Secur. Appl.* **2018**, *40*, 20–30. [CrossRef]
113. Pérez-González, D.; Preciado, S.T.; Solana-Gonzalez, P. Organizational Practices as Antecedents of the Information Security Management Performance. *Inf. Technol. People* **2019**, *32*, 1262–1275. [CrossRef]
114. Rebollo, O.; Mellado, D.; Fernández-Medina, E. A Systematic Review of Information Security Governance Frameworks in the Cloud Computing Environment. *J. Univers. Comput. Sci.* **2012**, *18*, 798–815. [CrossRef]
115. Arslan, O.; Çepni, M.S.; Etiler, N. Spatial Analysis of Perinatal Mortality Rates with Geographic Information Systems in Kocaeli, Turkey. *Public Health* **2013**, *127*, 369–379. [CrossRef]
116. Wu, D.; Wu, D.D. Risk-Based Robust Evaluation of Hospital Efficiency. *IEEE Syst. J.* **2019**, *13*, 1906–1914. [CrossRef]

117. Ben-Arieh, D.; Gullipalli, D.K. Data Envelopment Analysis of Clinics with Sparse Data: Fuzzy Clustering Approach. *Comput. Ind. Eng.* **2012**, *63*, 13–21. [CrossRef]
118. Verri Lucca, A.; Augusto Silva, L.; Luchtenberg, R.; Garcez, L.; Mao, X.; García Ovejero, R.; Miguel Pires, I.; Luis Victória Barbosa, J.; Reis Quietinho Leithardt, V. A Case Study on the Development of a Data Privacy Management Solution Based on Patient Information. *Sensors* **2020**, *20*, 6030. [CrossRef]
119. Golmohammadi, D.; Mellat-Parast, M. Developing a Grey-Based Decision-Making Model for Supplier Selection. *Int. J. Prod. Econ.* **2012**, *137*, 191–200. [CrossRef]
120. Ferdous, R.; Khan, F.; Sadiq, R.; Amyotte, P.; Veitch, B. Handling Data Uncertainties in Event Tree Analysis. *Process Saf. Environ. Prot.* **2009**, *87*, 283–292. [CrossRef]
121. Cao, Z.; Lumineau, F. Revisiting the Interplay between Contractual and Relational Governance: A Qualitative and Meta-Analytic Investigation. *J. Oper. Manag.* **2015**, *33–34*, 15–42. [CrossRef]
122. Liu, Q.; Zhou, T.; Cai, Z.; Yuan, Y.; Xu, M.; Qin, J.; Ma, W. Turning Backdoors for Efficient Privacy Protection against Image Retrieval Violations. *Inf. Process. Manag.* **2023**, *60*, 103471. [CrossRef]
123. Martin, K. The Penalty for Privacy Violations: How Privacy Violations Impact Trust Online. *J. Bus. Res.* **2018**, *82*, 103–116. [CrossRef]
124. Bansal, G.; Zahedi, F.M. Trust Violation and Repair: The Information Privacy Perspective. *Decis. Support Syst.* **2015**, *71*, 62–77. [CrossRef]
125. Melnik, T. Avoiding Violations of Patient Privacy With Social Media. *J. Nurs. Regul.* **2013**, *3*, 39–46. [CrossRef]
126. Liu, M.; Luo, Y.; Yang, C.; Pang, S.; Puthal, D.; Ren, K.; Zhang, X. Privacy-Preserving Matrix Product Based Static Mutual Exclusive Roles Constraints Violation Detection in Interoperable Role-Based Access Control. *Futur. Gener. Comput. Syst.* **2020**, *109*, 457–468. [CrossRef]
127. Tamjidyamcholo, A.; Bin Baba, M.S.; Shuib, N.L.M.; Rohani, V.A. Evaluation Model for Knowledge Sharing in Information Security Professional Virtual Community. *Comput. Secur.* **2014**, *43*, 19–34. [CrossRef]
128. Anwar, M.; He, W.; Ash, I.; Yuan, X.; Li, L.; Xu, L. Gender Difference and Employees' Cybersecurity Behaviors. *Comput. Hum. Behav.* **2017**, *69*, 437–443. [CrossRef]
129. Jalali, M.S.; Razak, S.; Gordon, W.; Perakslis, E.; Madnick, S. Health Care and Cybersecurity: Bibliometric Analysis of the Literature. *J. Med. Internet Res.* **2019**, *21*, e12644. [CrossRef]
130. Huber, T.L.; Fischer, T.A.; Dibbern, J.; Hirschheim, R. A Process Model of Complementarity and Substitution of Contractual and Relational Governance in IS Outsourcing. *J. Manag. Inf. Syst.* **2013**, *30*, 81–114. [CrossRef]
131. Manimaran, S.; Sastry, V.N.; Gopalan, N.P. SBTDDL: A Novel Framework for Sensor-Based Threats Detection on Android Smartphones Using Deep Learning. *Comput. Secur.* **2022**, *118*, 102729. [CrossRef]
132. Cano Bejar, A.H.; Ray, S.; Huang, Y.H. Fighting for the Status Quo: Threat to Tech Self-Esteem and Opposition to Competing Smartphones. *Inf. Manag.* **2023**, *60*, 103748. [CrossRef]
133. Tams, S.; Legoux, R.; Léger, P.-M. Smartphone Withdrawal Creates Stress: A Moderated Mediation Model of Nomophobia, Social Threat, and Phone Withdrawal Context. *Comput. Hum. Behav.* **2018**, *81*, 1–9. [CrossRef]
134. Pang, H.; Ruan, Y. Can Information and Communication Overload Influence Smartphone App Users' Social Network Exhaustion, Privacy Invasion and Discontinuance Intention? A Cognition-Affect-Conation Approach. *J. Retail. Consum. Serv.* **2023**, *73*, 103378. [CrossRef]
135. De Prisco, R.; De Santis, A.; Malandrino, D.; Zaccagnino, R. An Improved Privacy Attack on Smartphones Exploiting the Accelerometer. *J. Inf. Secur. Appl.* **2023**, *75*, 103479. [CrossRef]
136. Nepomuceno, T.C.C. Parametric and Non-Parametric Data-Driven Analytics for Socioeconomic Challenges in a Contemporary World. *Socioecon. Anal.* **2023**, *1*, 1–4. [CrossRef]
137. De Carvalho, V.D.H.; Costa, A.P.C.S. Exploring Text Mining and Analytics for Applications in Public Security: An in-Depth Dive into a Systematic Literature Review. *Socioecon. Anal.* **2023**, *1*, 5–55. [CrossRef]
138. Sanchez, P.M.S.; Valero, J.M.J.; Celdran, A.H.; Bovet, G.; Perez, M.G.; Perez, G.M. A Survey on Device Behavior Fingerprinting: Data Sources, Techniques, Application Scenarios, and Datasets. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 1048–1077. [CrossRef]
139. Jimada-Ojuolape, B.; Teh, J. Surveys on the Reliability Impacts of Power System Cyber–Physical Layers. *Sustain. Cities Soc.* **2020**, *62*, 102384. [CrossRef]
140. Kim, K.; Kim, J.S.; Jeong, S.; Park, J.-H.; Kim, H.K. Cybersecurity for Autonomous Vehicles: Review of Attacks and Defense. *Comput. Secur.* **2021**, *103*, 102150. [CrossRef]
141. Alotaibi, A.; Barnawi, A. Securing Massive IoT in 6G: Recent Solutions, Architectures, Future Directions. *Internet Things* **2023**, *22*, 100715. [CrossRef]
142. Raimundo, R.J.; Rosário, A.T. Cybersecurity in the Internet of Things in Industrial Management. *Appl. Sci.* **2022**, *12*, 1598. [CrossRef]
143. Yang, F.; Hua, Y.; Li, X.; Yang, Z.; Yu, X.; Fei, T. A Survey on Multisource Heterogeneous Urban Sensor Access and Data Management Technologies. *Meas. Sens.* **2022**, *19*, 100061. [CrossRef]
144. van Eck, N.J.; Waltman, L.; Dekker, R.; van den Berg, J. A Comparison of Two Techniques for Bibliometric Mapping: Multidimensional Scaling and VOS. *J. Am. Soc. Inf. Sci. Technol.* **2010**, *61*, 2405–2416. [CrossRef]
145. Chou Yen, D.; Lin, B.; Hong-Lam, C.P.D. Cyberspace Security Management. *Ind. Manag. Data Syst.* **1999**, *99*, 353–361. [CrossRef]

146. Nepomuceno, T.C.C.; Piubello Orsini, L.; de Carvalho, V.D.H.; Poleto, T.; Leardini, C. The Core of Healthcare Efficiency: A Comprehensive Bibliometric Review on Frontier Analysis of Hospitals. *Healthcare* **2022**, *10*, 1316. [CrossRef]
147. van Eck, N.J.; Waltman, L. Visualizing Bibliometric Networks. In *Measuring Scholarly Impact*; Ding, Y., Rousseau, R., Wolfram, D., Eds.; Springer International Publishing: Cham, Switzerland, 2014; pp. 285–320. ISBN 978-3-319-10377-8.
148. van Eck, N.J.; Waltman, L. Software Survey: VOSviewer, a Computer Program for Bibliometric Mapping. *Scientometrics* **2010**, *84*, 523–538. [CrossRef]
149. Satarova, B.; Siddiqui, T.; Raza, H.; Abbasi, N.; Kydyrkozha, S. A Systematic Review of "The Performance of Knowledge Organizations and Modelling Human Action". *Socioecon. Anal.* **2023**, *1*, 56–77. [CrossRef]
150. Ahmad, F.; Adnane, A.; Franqueira, V.; Kurugollu, F.; Liu, L. Man-In-The-Middle Attacks in Vehicular Ad-Hoc Networks: Evaluating the Impact of Attackers' Strategies. *Sensors* **2018**, *18*, 4040. [CrossRef]
151. Abi Sen, A.A.; Eassa, F.A.; Jambi, K.; Yamin, M. Preserving Privacy in Internet of Things: A Survey. *Int. J. Inf. Technol.* **2018**, *10*, 189–200. [CrossRef]
152. Ahmad, F.; Franqueira, V.N.L.; Adnane, A. TEAM: A Trust Evaluation and Management Framework in Context-Enabled Vehicular Ad-Hoc Networks. *IEEE Access* **2018**, *6*, 28643–28660. [CrossRef]
153. Ahmad, F.; Kurugollu, F.; Adnane, A.; Hussain, R.; Hussain, F. MARINE: Man-in-the-Middle Attack Resistant Trust Model in Connected Vehicles. *IEEE Internet Things J.* **2020**, *7*, 3310–3322. [CrossRef]
154. Ahmad, F.; Kurugollu, F.; Kerrache, C.A.; Sezer, S.; Liu, L. NOTRINO: A NOvel Hybrid TRust Management Scheme for INternet-of-Vehicles. *IEEE Trans. Veh. Technol.* **2021**, *70*, 9244–9257. [CrossRef]
155. Farahani, B.; Firouzi, F.; Chang, V.; Badaroglu, M.; Constant, N.; Mankodiya, K. Towards Fog-Driven IoT EHealth: Promises and Challenges of IoT in Medicine and Healthcare. *Futur. Gener. Comput. Syst.* **2018**, *78*, 659–676. [CrossRef]
156. Gaba, G.S.; Hedabou, M.; Kumar, P.; Braeken, A.; Liyanage, M.; Alazab, M. Zero Knowledge Proofs Based Authenticated Key Agreement Protocol for Sustainable Healthcare. *Sustain. Cities Soc.* **2022**, *80*, 103766. [CrossRef]
157. Javed, M.; Ben Hamida, E.; Znaidi, W. Security in Intelligent Transport Systems for Smart Cities: From Theory to Practice. *Sensors* **2016**, *16*, 879. [CrossRef]
158. Garcia-Font, V.; Garrigues, C.; Rifà-Pous, H. A Comparative Study of Anomaly Detection Techniques for Smart City Wireless Sensor Networks. *Sensors* **2016**, *16*, 868. [CrossRef]
159. Garcia-Font, V.; Garrigues, C.; Rifà-Pous, H. Attack Classification Schema for Smart City WSNs. *Sensors* **2017**, *17*, 771. [CrossRef]
160. Beltran, V.; Skarmeta, A.F.; Ruiz, P.M. An ARM-Compliant Architecture for User Privacy in Smart Cities: SMARTIE—Quality by Design in the IoT. *Wirel. Commun. Mob. Comput.* **2017**, *2017*, 1–13. [CrossRef]
161. Chatzigiannakis, I.; Vitaletti, A.; Pyrgelis, A. A Privacy-Preserving Smart Parking System Using an IoT Elliptic Curve Based Security Platform. *Comput. Commun.* **2016**, *89–90*, 165–177. [CrossRef]
162. Chen, C.-T.; Lee, C.-C.; Lin, I.-C. Efficient and Secure Three-Party Mutual Authentication Key Agreement Protocol for WSNs in IoT Environments. *PLoS ONE* **2020**, *15*, e0232277. [CrossRef]
163. Das, A.K.; Bera, B.; Wazid, M.; Jamal, S.S.; Park, Y. On the Security of a Secure and Lightweight Authentication Scheme for Next Generation IoT Infrastructure. *IEEE Access* **2021**, *9*, 71856–71867. [CrossRef]
164. Jain, S.K.; Kesswani, N.; Agarwal, B. Security, Privacy and Trust: Privacy Preserving Model for Internet of Things. *Int. J. Intell. Inf. Database Syst.* **2020**, *13*, 249. [CrossRef]
165. Kamil, I.A.; Ogundoyin, S.O. A Big Data Anonymous Batch Verification Scheme with Conditional Privacy Preservation for Power Injection over Vehicular Network and 5G Smart Grid Slice. *Sustain. Energy Grids Netw.* **2019**, *20*, 100260. [CrossRef]
166. Singh, S.; Pise, A.; Alfarraj, O.; Tolba, A.; Yoon, B. A Cryptographic Approach to Prevent Network Incursion for Enhancement of QoS in Sustainable Smart City Using MANET. *Sustain. Cities Soc.* **2022**, *79*, 103483. [CrossRef]
167. Khan, Z.A. Using Energy-Efficient Trust Management to Protect IoT Networks for Smart Cities. *Sustain. Cities Soc.* **2018**, *40*, 1–15. [CrossRef]
168. Li, X.; Shen, X. Blockchain Technology-Based Electronic Payment Strategy for City Mobile Pass Cards. *Mob. Inf. Syst.* **2022**, *2022*, 4085036. [CrossRef]
169. Garcia-Font, V. SocialBlock: An Architecture for Decentralized User-Centric Data Management Applications for Communications in Smart Cities. *J. Parallel Distrib. Comput.* **2020**, *145*, 13–23. [CrossRef]
170. Gong, B.; Liu, J.; Guo, S. A Trusted Attestation Scheme for Data Source of Internet of Things in Smart City Based on Dynamic Trust Classification. *IEEE Internet Things J.* **2021**, *8*, 16121–16141. [CrossRef]
171. Ghahramani, M.; Javidan, R.; Shojafar, M. A Secure Biometric-Based Authentication Protocol for Global Mobility Networks in Smart Cities. *J. Supercomput.* **2020**, *76*, 8729–8755. [CrossRef]
172. Gaur, M.S.; Kumar, S.; Gaur, N.K.; Sharma, P.S. Persuasive Factors and Weakness for Security Vulnerabilities in BIG IOT Data in Healthcare Solution. *J. Phys. Conf. Ser.* **2021**, *2007*, 12046. [CrossRef]
173. Gope, P.; Amin, R.; Hafizul Islam, S.K.; Kumar, N.; Bhalla, V.K. Lightweight and Privacy-Preserving RFID Authentication Scheme for Distributed IoT Infrastructure with Secure Localization Services for Smart City Environment. *Futur. Gener. Comput. Syst.* **2018**, *83*, 629–637. [CrossRef]
174. Islam, S.K.H.; Obaidat, M.S.; Vijayakumar, P.; Abdulhay, E.; Li, F.; Reddy, M.K.C. A Robust and Efficient Password-Based Conditional Privacy Preserving Authentication and Group-Key Agreement Protocol for VANETs. *Futur. Gener. Comput. Syst.* **2018**, *84*, 216–227. [CrossRef]

175. Hassan, A.M.; Awad, A.I. Urban Transition in the Era of the Internet of Things: Social Implications and Privacy Challenges. *IEEE Access* **2018**, *6*, 36428–36440. [CrossRef]
176. Kumar, A.; Abhishek, K.; Liu, X.; Haldorai, A. An Efficient Privacy-Preserving ID Centric Authentication in IoT Based Cloud Servers for Sustainable Smart Cities. *Wirel. Pers. Commun.* **2021**, *117*, 3229–3253. [CrossRef]
177. Lee, J.; Kim, G.; Das, A.K.; Park, Y. Secure and Efficient Honey List-Based Authentication Protocol for Vehicular Ad Hoc Networks. *IEEE Trans. Netw. Sci. Eng.* **2021**, *8*, 2412–2425. [CrossRef]
178. Li, X.; Liu, T.; Obaidat, M.S.; Wu, F.; Vijayakumar, P.; Kumar, N. A Lightweight Privacy-Preserving Authentication Protocol for VANETs. *IEEE Syst. J.* **2020**, *14*, 3547–3557. [CrossRef]
179. Li, X.; Sangaiah, A.K.; Kumari, S.; Wu, F.; Shen, J.; Khan, M.K. An Efficient Authentication and Key Agreement Scheme with User Anonymity for Roaming Service in Smart City. *Pers. Ubiquitous Comput.* **2017**, *21*, 791–805. [CrossRef]
180. Liu, W.; Wang, X.; Peng, W. Secure Remote Multi-Factor Authentication Scheme Based on Chaotic Map Zero-Knowledge Proof for Crowdsourcing Internet of Things. *IEEE Access* **2020**, *8*, 8754–8767. [CrossRef]
181. Malik, V.; Singh, S. Security Risk Management in IoT Environment. *J. Discret. Math. Sci. Cryptogr.* **2019**, *22*, 697–709. [CrossRef]
182. Khattak, H.A.; Farman, H.; Jan, B.; Din, I.U. Toward Integrating Vehicular Clouds with IoT for Smart City Services. *IEEE Netw.* **2019**, *33*, 65–71. [CrossRef]
183. Rauf, A.; Wang, Z.; Sajid, H.; Ali Tahir, M. Secure Route-Obfuscation Mechanism with Information-Theoretic Security for Internet of Things. *Sensors* **2020**, *20*, 4221. [CrossRef] [PubMed]
184. Qureshi, K.N.; Qayyum, S.; Ul Islam, M.N.; Jeon, G. A Secure Data Parallel Processing Based Embedded System for Internet of Things Computer Vision Using Field Programmable Gate Array Devices. *Int. J. Circuit Theory Appl.* **2021**, *49*, 1450–1469. [CrossRef]
185. Salameh, H.B.; Almajali, S.; Ayyash, M.; Elgala, H. Security-Aware Channel Assignment in IoT-Based Cognitive Radio Networks for Time-Critical Applications. In Proceedings of the 2017 Fourth International Conference on Software Defined Systems (SDS), Valencia, Spain, 8–11 May 2017; IEEE: New York, NY, USA, 2017; pp. 43–47.
186. Reddy, A.G.; Suresh, D.; Phaneendra, K.; Shin, J.S.; Odelu, V. Provably Secure Pseudo-Identity Based Device Authentication for Smart Cities Environment. *Sustain. Cities Soc.* **2018**, *41*, 878–885. [CrossRef]
187. Liu, X.; Wang, J.; Yang, Y.; Cao, Z.; Xiong, G.; Xia, W. Inferring Behaviors via Encrypted Video Surveillance Traffic by Machine Learning. In Proceedings of the 2019 IEEE 21st International Conference on High Performance Computing and Communications, IEEE 17th International Conference on Smart City, IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Zhangjiajie, China, 10–12 August 2019; IEEE: New York, NY, USA, 2019; pp. 273–280.
188. Memos, V.A.; Psannis, K.E.; Ishibashi, Y.; Kim, B.-G.; Gupta, B.B. An Efficient Algorithm for Media-Based Surveillance System (EAMSuS) in IoT Smart City Framework. *Futur. Gener. Comput. Syst.* **2018**, *83*, 619–628. [CrossRef]
189. Mohanta, B.K.; Jena, D.; Satapathy, U.; Ramasubbareddy, S. Collaborative Decision Making System in Intelligent Transportation System Using Distributed Blockchain Technology. *Int. J. Veh. Inf. Commun. Syst.* **2022**, *7*, 64. [CrossRef]
190. Meshram, C.; Ibrahim, R.W.; Deng, L.; Shende, S.W.; Meshram, S.G.; Barve, S.K. A Robust Smart Card and Remote User Password-Based Authentication Protocol Using Extended Chaotic Maps under Smart Cities Environment. *Soft Comput.* **2021**, *25*, 10037–10051. [CrossRef]
191. Zakaria, H.; Abu Bakar, N.A.; Hassan, N.H.; Yaacob, S. IoT Security Risk Management Model for Secured Practice in Healthcare Environment. *Procedia Comput. Sci.* **2019**, *161*, 1241–1248. [CrossRef]
192. Pangestuti, D.D.; Susanto, T.D.; Trisunarno, L. Measuring Smart Cities: Identification of Smart Society Indicators in Indonesia. In Proceedings of the 2021 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Kuala Lumpur, Malaysia, 12–16 December 2021; IEEE: New York, NY, USA, 2021; pp. 1245–1249.
193. Nikooghadam, M.; Amintoosi, H.; Islam, S.K.H.; Moghadam, M.F. A Provably Secure and Lightweight Authentication Scheme for Internet of Drones for Smart City Surveillance. *J. Syst. Archit.* **2021**, *115*, 101955. [CrossRef]
194. Tanveer, M.; Khan, A.U.; Shah, H.; Chaudhry, S.A.; Naushad, A. PASKE-IoD: Privacy-Protecting Authenticated Key Establishment for Internet of Drones. *IEEE Access* **2021**, *9*, 145683–145698. [CrossRef]
195. Tamizharasi, G.S.; Sultanah, H.P.; Balamurugan, B. IoT-Based E-Health System Security: A Vision Archictecture Elements and Future Directions. In Proceedings of the 2017 International Conference of Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 20–22 April 2017; IEEE: New York, NY, USA, 2017; pp. 655–661.
196. Verde, L.; De Pietro, G.; Alrashoud, M.; Ghoneim, A.; Al-Mutib, K.N.; Sannino, G. Leveraging Artificial Intelligence to Improve Voice Disorder Identification Through the Use of a Reliable Mobile App. *IEEE Access* **2019**, *7*, 124048–124054. [CrossRef]
197. Wazid, M.; Das, A.K.; Bhat, K.V.; Vasilakos, A.V. LAM-CIoT: Lightweight Authentication Mechanism in Cloud-Based IoT Environment. *J. Netw. Comput. Appl.* **2020**, *150*, 102496. [CrossRef]
198. Umar, M.; Islam, S.K.H.; Mahmood, K.; Ahmed, S.; Ghaffar, Z.; Saleem, M.A. Provable Secure Identity-Based Anonymous and Privacy-Preserving Inter-Vehicular Authentication Protocol for VANETS Using PUF. *IEEE Trans. Veh. Technol.* **2021**, *70*, 12158–12167. [CrossRef]
199. Wu, F.; Li, X.; Xu, L.; Kumari, S.; Lin, D.; Rodrigues, J.J.P.C. An Anonymous and Identity-Trackable Data Transmission Scheme for Smart Grid under Smart City Notion. *Ann. Telecommun.* **2020**, *75*, 307–317. [CrossRef]
200. Bagga, P.; Sutrala, A.K.; Das, A.K.; Vijayakumar, P. Blockchain-Based Batch Authentication Protocol for Internet of Vehicles. *J. Syst. Archit.* **2021**, *113*, 101877. [CrossRef]

201. Vijayakumar, P.; Azees, M.; Chang, V.; Deborah, J.; Balusamy, B. Computationally Efficient Privacy Preserving Authentication and Key Distribution Techniques for Vehicular Ad Hoc Networks. *Clust. Comput.* **2017**, *20*, 2439–2450. [CrossRef]
202. Wu, F.; Li, X.; Xu, L.; Kumari, S. A Privacy-Preserving Scheme with Identity Traceable Property for Smart Grid. *Comput. Commun.* **2020**, *157*, 38–44. [CrossRef]
203. Sutrala, A.K.; Obaidat, M.S.; Saha, S.; Das, A.K.; Alazab, M.; Park, Y. Authenticated Key Agreement Scheme With User Anonymity and Untraceability for 5G-Enabled Softwarized Industrial Cyber-Physical Systems. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 2316–2330. [CrossRef]
204. Sharma, G.; Kalra, S. Advanced Multi-Factor User Authentication Scheme for E-Governance Applications in Smart Cities. *Int. J. Comput. Appl.* **2019**, *41*, 312–327. [CrossRef]
205. Simic, M.; Stankovic, M.; Orlic, V.D. Physical Layer Communication Security in Smart Cities: Challenges and Threats Identification. In Proceedings of the 2021 15th International Conference on Advanced Technologies, Systems and Services in Telecommunications (TELSIKS), Nis, Serbia, 20–22 October 2021; IEEE: New York, NY, USA, 2021; pp. 209–218.
206. Hamalainen, M.; Tyrvainen, P. A Framework for IoT Service Experiment Platforms in Smart-City Environments. In Proceedings of the 2016 IEEE International Smart Cities Conference (ISC2), Trento, Italy, 12–15 September 2016; IEEE: New York, NY, USA, 2016; pp. 1–8.
207. Taher, B.H.; Liu, H.; Abedi, F.; Lu, H.; Yassin, A.A.; Mohammed, A.J. A Secure and Lightweight Three-Factor Remote User Authentication Protocol for Future IoT Applications. *J. Sens.* **2021**, *2021*, 8871204. [CrossRef]
208. Sylla, T.; Chalouf, M.A.; Krief, F.; Samaké, K. SETUCOM: Secure and Trustworthy Context Management for Context-Aware Security and Privacy in the Internet of Things. *Secur. Commun. Netw.* **2021**, *2021*, 6632747. [CrossRef]
209. Xie, Q.; Hwang, L. Security Enhancement of an Anonymous Roaming Authentication Scheme with Two-Factor Security in Smart City. *Neurocomputing* **2019**, *347*, 131–138. [CrossRef]
210. Wu, H.; Li, L.; Liu, Y.; Wu, X. Vehicle-Based Secure Location Clustering for IoT-Equipped Building and Facility Management in Smart City. *Build. Environ.* **2022**, *214*, 108937. [CrossRef]
211. Sanober, S.; Aldawsari, M.; Karimovna, A.D.; Ofori, I. Blockchain Integrated with Principal Component Analysis: A Solution to Smart Security against Cyber-Attacks. *Secur. Commun. Netw.* **2022**, *2022*, 8649060. [CrossRef]
212. Zhang, J.; Zong, Y.; Yang, C.; Miao, Y.; Guo, J. LBOA: Location-Based Secure Outsourced Aggregation in IoT. *IEEE Access* **2019**, *7*, 43869–43883. [CrossRef]
213. Zhang, H.; Babar, M.; Tariq, M.U.; Jan, M.A.; Menon, V.G.; Li, X. SafeCity: Toward Safe and Secured Data Management Design for IoT-Enabled Smart City Planning. *IEEE Access* **2020**, *8*, 145256–145267. [CrossRef]
214. Wei, C. Copyright Protection and Data Reliability of AI-Written Literary Creations in Smart City. *Secur. Commun. Netw.* **2022**, *2022*, 6498468. [CrossRef]
215. Banerjee, S.; Odelu, V.; Das, A.K.; Srinivas, J.; Kumar, N.; Chattopadhyay, S.; Choo, K.-K.R. A Provably Secure and Lightweight Anonymous User Authenticated Session Key Exchange Scheme for Internet of Things Deployment. *IEEE Internet Things J.* **2019**, *6*, 8739–8752. [CrossRef]
216. Haseeb, K.; Ud Din, I.; Almogren, A.; Ahmed, I.; Guizani, M. Intelligent and Secure Edge-Enabled Computing Model for Sustainable Cities Using Green Internet of Things. Sustain. *Cities Soc.* **2021**, *68*, 102779. [CrossRef]
217. Lever, K.E.; Kifayat, K. Identifying and Mitigating Security Risks for Secure and Robust NGI Networks. *Sustain. Cities Soc.* **2020**, *59*, 102098. [CrossRef]
218. Mishra, A.K.; Puthal, D.; Tripathy, A.K. GraphCrypto: Next Generation Data Security Approach towards Sustainable Smart City Building. *Sustain. Cities Soc.* **2021**, *72*, 103056. [CrossRef]
219. Wang, Z.; Jiang, D.; Wang, F.; Lv, Z.; Nowak, R. A Polymorphic Heterogeneous Security Architecture for Edge-Enabled Smart Grids. *Sustain. Cities Soc.* **2021**, *67*, 102661. [CrossRef]
220. Duraisamy, A.; Subramaniam, M. Attack Detection on IoT Based Smart Cities Using IDS Based MANFIS Classifier and Secure Data Transmission Using IRSA Encryption. *Wirel. Pers. Commun.* **2021**, *119*, 1913–1934. [CrossRef]
221. Deebak, B.D.; AL-Turjman, F. A Robust and Distributed Architecture for 5G-Enabled Networks in the Smart Blockchain Era. *Comput. Commun.* **2022**, *181*, 293–308. [CrossRef]
222. Dwivedi, S.K.; Amin, R.; Vollala, S.; Chaudhry, R. Blockchain-Based Secured Event-Information Sharing Protocol in Internet of Vehicles for Smart Cities. *Comput. Electr. Eng.* **2020**, *86*, 106719. [CrossRef]
223. Ferreira, C.M.S.; Garrocho, C.T.B.; Oliveira, R.A.R.; Silva, J.S.; Cavalcanti, C.F.M.D.C. IoT Registration and Authentication in Smart City Applications with Blockchain. *Sensors* **2021**, *21*, 1323. [CrossRef]
224. Guan, Z.; Si, G.; Zhang, X.; Wu, L.; Guizani, N.; Du, X.; Ma, Y. Privacy-Preserving and Efficient Aggregation Based on Blockchain for Power Grid Communications in Smart Communities. *IEEE Commun. Mag.* **2018**, *56*, 82–88. [CrossRef]
225. Esposito, C.; Ficco, M.; Gupta, B.B. Blockchain-Based Authentication and Authorization for Smart City Applications. *Inf. Process. Manag.* **2021**, *58*, 102468. [CrossRef]
226. Kumari, A.; Tanwar, S. Secure Data Analytics for Smart Grid Systems in a Sustainable Smart City: Challenges, Solutions, and Future Directions. *Sustain. Comput. Inform. Syst.* **2020**, *28*, 100427. [CrossRef]
227. Kuppa, K.; Dayal, A.; Gupta, S.; Dua, A.; Chaudhary, P.; Rathore, S. ConvXSS: A Deep Learning-Based Smart ICT Framework against Code Injection Attacks for HTML5 Web Applications in Sustainable Smart City Infrastructure. *Sustain. Cities Soc.* **2022**, *80*, 103765. [CrossRef]

228. Kumari, A.; Gupta, R.; Tanwar, S. Amalgamation of Blockchain and IoT for Smart Cities Underlying 6G Communication: A Comprehensive Review. *Comput. Commun.* **2021**, *172*, 102–118. [CrossRef]
229. Ma, C.; Zeng, S.; Li, D. A New Algorithm for Backlight Image Enhancement. In Proceedings of the 2020 International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS), Vientiane, Laos, 11–12 January 2020; IEEE: New York, NY, USA, 2020; pp. 840–844.
230. Ma, R.; Lam, P.T.I.; Leung, C.K. Reliability Analysis of a Smart Parking Information System: The Case of Hong Kong. *Wirel. Pers. Commun.* **2021**, *119*, 1681–1701. [CrossRef]
231. Gohari, S.; Ahlers, D.F.; Nielsen, B.; Junker, E. The Governance Approach of Smart City Initiatives. Evidence from Trondheim, Bergen, and Bodø. *Infrastructures* **2020**, *5*, 31. [CrossRef]
232. Huang, C.-Y.; Chiang, Y.-H.; Tsai, F. An Ontology Integrating the Open Standards of City Models and Internet of Things for Smart-City Applications. *IEEE Internet Things J.* **2022**, *9*, 20444–20457. [CrossRef]
233. Huh, J.-H.; Kim, S.-K. The Blockchain Consensus Algorithm for Viable Management of New and Renewable Energies. *Sustainability* **2019**, *11*, 3184. [CrossRef]
234. Jamil, F.; Cheikhrouhou, O.; Jamil, H.; Koubaa, A.; Derhab, A.; Ferrag, M.A. PetroBlock: A Blockchain-Based Payment Mechanism for Fueling Smart Vehicles. *Appl. Sci.* **2021**, *11*, 3055. [CrossRef]
235. Kamal, R.; Hemdan, E.E.; El-Fishway, N. Forensics Chain for Evidence Preservation System: An Evidence Preservation Forensics Framework for Internet of Things-based Smart City Security Using Blockchain. *Concurr. Comput. Pract. Exp.* **2022**, *34*, e7062. [CrossRef]
236. Khan, Z.; Abbasi, A.G.; Pervez, Z. Blockchain and Edge Computing–Based Architecture for Participatory Smart City Applications. *Concurr. Comput. Pract. Exp.* **2020**, *32*, e5566. [CrossRef]
237. Jan, A.; Parah, S.A.; Malik, B.A. IEFHAC: Image Encryption Framework Based on Hessenberg Transform and Chaotic Theory for Smart Health. *Multimed. Tools Appl.* **2022**, *81*, 18829–18853. [CrossRef] [PubMed]
238. Roldán-Gómez, J.J.; Garcia-Aunon, P.; Mazariegos, P.; Barrientos, A. SwarmCity Project: Monitoring Traffic, Pedestrians, Climate, and Pollution with an Aerial Robotic Swarm. *Pers. Ubiquitous Comput.* **2022**, *26*, 1151–1167. [CrossRef]
239. Salkuti, S.R. Smart Cities: Understanding Policies, Standards, Applications and Case Studies. *Int. J. Electr. Comput. Eng.* **2021**, *11*, 3137. [CrossRef]
240. Sharma, P.K.; Ryu, J.H.; Park, K.Y.; Park, J.H.; Park, J.H. Li-Fi Based on Security Cloud Framework for Future IT Environment. *Hum. Centric Comput. Inf. Sci.* **2018**, *8*, 23. [CrossRef]
241. Mukherjee, A.; Sahoo, S.; Halder, R. A Blockchain-Based Integrated and Interconnected Hybrid Platform for Smart City Ecosystem. *Peer Peer Netw. Appl.* **2022**, *15*, 2116–2141. [CrossRef]
242. Singh, S.K.; Rathore, S.; Park, J.H. Block IoT Intelligence: A Blockchain-Enabled Intelligent IoT Architecture with Artificial Intelligence. *Futur. Gener. Comput. Syst.* **2020**, *110*, 721–743. [CrossRef]
243. Otuoze, A.O.; Mustafa, M.W.; Mohammed, O.O.; Saeed, M.S.; Surajudeen-Bakinde, N.T.; Salisu, S. Electricity Theft Detection by Sources of Threats for Smart City Planning. *IET Smart Cities* **2019**, *1*, 52–60. [CrossRef]
244. Omar, A.; Al Jamil, A.K.; Khandakar, A.; Uzzal, A.R.; Bosri, R.; Mansoor, N.; Rahman, M.S. A Transparent and Privacy-Preserving Healthcare Platform With Novel Smart Contract for Smart Cities. *IEEE Access* **2021**, *9*, 90738–90749. [CrossRef]
245. Joshi, S.; Dubey, D.M.; Kumar Mishra, D.D. An Approach Using Trust Management with Next-Generation IoT Networks for Healthcare, Agriculture and Sustainable Development Goals. *J. Univ. Shanghai Sci. Technol.* **2021**, *23*, 87. [CrossRef]
246. Pujol, F.A.; Mora, H.; Pertegal, M.L. A Soft Computing Approach to Violence Detection in Social Media for Smart Cities. *Soft Comput.* **2020**, *24*, 11007–11017. [CrossRef]
247. Rehman, A.; Haseeb, K.; Saba, T.; Kolivand, H. M-SMDM: A Model of Security Measures Using Green Internet of Things with Cloud Integrated Data Management for Smart Cities. *Environ. Technol. Innov.* **2021**, *24*, 101802. [CrossRef]
248. Pereira, J.; Batista, T.; Cavalcante, E.; Souza, A.; Lopes, F.; Cacho, N. A Platform for Integrating Heterogeneous Data and Developing Smart City Applications. *Futur. Gener. Comput. Syst.* **2022**, *128*, 552–566. [CrossRef]
249. Alonso, Á.; Fernández, F.; Marco, L.; Salvachúa, J. IAACaaS: IoT Application-Scoped Access Control as a Service. *Futur. Internet* **2017**, *9*, 64. [CrossRef]
250. Yuvaraj, N.; Praghash, K.; Raja, R.A.; Karthikeyan, T. An Investigation of Garbage Disposal Electric Vehicles (GDEVs) Integrated with Deep Neural Networking (DNN) and Intelligent Transportation System (ITS) in Smart City Management System (SCMS). *Wirel. Pers. Commun.* **2022**, *123*, 1733–1752. [CrossRef]
251. Wang, D.; Bai, B.; Lei, K.; Zhao, W.; Yang, Y.; Han, Z. Enhancing Information Security via Physical Layer Approaches in Heterogeneous IoT With Multiple Access Mobile Edge Computing in Smart City. *IEEE Access* **2019**, *7*, 54508–54521. [CrossRef]
252. Xie, J.; Tang, H.; Huang, T.; Yu, F.R.; Xie, R.; Liu, J.; Liu, Y. A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2794–2830. [CrossRef]
253. Xu, Z.; Luo, M.; Vijayakumar, P.; Peng, C.; Wang, L. Efficient Certificateless Designated Verifier Proxy Signature Scheme Using UAV Network for Sustainable Smart City. *Sustain. Cities Soc.* **2022**, *80*, 103771. [CrossRef]
254. Xu, R.; Chen, Y. Fed-DDM: A Federated Ledgers Based Framework for Hierarchical Decentralized Data Marketplaces. In Proceedings of the 2021 International Conference on Computer Communications and Networks (ICCCN), Athens, Greece, 19–22 July 2021; IEEE: New York, NY, USA, 2021; pp. 1–8.

255. Yazdinejad, A.; Srivastava, G.; Parizi, R.M.; Dehghantanha, A.; Choo, K.-K.R.; Aledhari, M. Decentralized Authentication of Distributed Patients in Hospital Networks Using Blockchain. *IEEE J. Biomed. Heal. Inform.* **2020**, *24*, 2146–2156. [CrossRef] [PubMed]
256. Yahaya, A.S.; Javaid, N.; Javed, M.U.; Shafiq, M.; Khan, W.Z.; Aalsalem, M.Y. Blockchain-Based Energy Trading and Load Balancing Using Contract Theory and Reputation in a Smart Community. *IEEE Access* **2020**, *8*, 222168–222186. [CrossRef]
257. Al-Aswad, H.; El-Medany, W.M.; Balakrishna, C.; Ababneh, N.; Curran, K. BZKP: Blockchain-Based Zero-Knowledge Proof Model for Enhancing Healthcare Security in Bahrain IoT Smart Cities and COVID-19 Risk Mitigation. *Arab J. Basic Appl. Sci.* **2021**, *28*, 154–171. [CrossRef]
258. Al-Muhtadi, J.; Saleem, K.; Al-Rabiaah, S.; Imran, M.; Gawanmeh, A.; Rodrigues, J.J.P.C. A Lightweight Cyber Security Framework with Context-Awareness for Pervasive Computing Environments. *Sustain. Cities Soc.* **2021**, *66*, 102610. [CrossRef]
259. Alasbali, N.; Azzuhri, S.R.B.; Salleh, R.B.; Kiah, M.L.M.; Shariffuddin, A.A.A.S.A.; Kamel, N.M.I.B.N.M.; Ismail, L. Rules of Smart IoT Networks within Smart Cities towards Blockchain Standardization. *Mob. Inf. Syst.* **2022**, *2022*, 9109300. [CrossRef]
260. Alasbali, N.; Azzuhri, S.R.B.; Salleh, R. Stakeholders' Viewpoints toward Blockchain Integration within IoT-Based Smart Cities. *J. Sens.* **2021**, *2021*, 4680021. [CrossRef]
261. Alharthi, A.; Ni, Q.; Jiang, R. A Privacy-Preservation Framework Based on Biometrics Blockchain (BBC) to Prevent Attacks in VANET. *IEEE Access* **2021**, *9*, 87299–87309. [CrossRef]
262. Abishu, H.N.; Seid, A.M.; Yacob, Y.H.; Ayall, T.; Sun, G.; Liu, G. Consensus Mechanism for Blockchain-Enabled Vehicle-to-Vehicle Energy Trading in the Internet of Electric Vehicles. *IEEE Trans. Veh. Technol.* **2022**, *71*, 946–960. [CrossRef]
263. Abbas, K.; Tawalbeh, L.A.; Rafiq, A.; Muthanna, A.; Elgendy, I.A.; Abd El-Latif, A.A. Convergence of Blockchain and IoT for Secure Transportation Systems in Smart Cities. *Secur. Commun. Netw.* **2021**, *2021*, 5597679. [CrossRef]
264. Abou-Nassar, E.M.; Iliyasu, A.M.; El-Kafrawy, P.M.; Song, O.-Y.; Bashir, A.K.; El-Latif, A.A.A. DITrust Chain: Towards Blockchain-Based Trust Models for Sustainable Healthcare IoT Systems. *IEEE Access* **2020**, *8*, 111223–111238. [CrossRef]
265. Chaudhary, R.; Jindal, A.; Aujla, G.S.; Aggarwal, S.; Kumar, N.; Choo, K.-K.R. BEST: Blockchain-Based Secure Energy Trading in SDN-Enabled Intelligent Transportation System. *Comput. Secur.* **2019**, *85*, 288–299. [CrossRef]
266. Cha, J.; Singh, S.K.; Kim, T.W.; Park, J.H. Blockchain-Empowered Cloud Architecture Based on Secret Sharing for Smart City. *J. Inf. Secur. Appl.* **2021**, *57*, 102686. [CrossRef]
267. Botello, J.V.; Mesa, A.P.; Rodríguez, F.A.; Díaz-López, D.; Nespoli, P.; Mármol, F.G. BlockSIEM: Protecting Smart City Services through a Blockchain-Based and Distributed SIEM. *Sensors* **2020**, *20*, 4636. [CrossRef]
268. Dar, M.A.; Askar, A.; Bhat, S.A. Blockchain Based Secure Data Exchange between Cloud Networks and Smart Hand-Held Devices for Use in Smart Cities. In Proceedings of the 2022 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), Jeju Island, Republic of Korea, 21–24 February 2022; IEEE: New York, NY, USA, 2022; pp. 457–460.
269. Alsaffar, N.; Medany, W.M.; El Ali, H. Low Complexity Cybersecurity Architecture for the Development of ITS in Smart Cities. *Int. J. Electron. Secur. Digit. Forensics* **2021**, *13*, 571. [CrossRef]
270. Alsammak, I.L.H.; Alomari, M.F.; Shakir Nasir, I.; Itwee, W.H. A Model for Blockchain-Based Privacy-Preserving for Big Data Users on the Internet of Thing. *Indones. J. Electr. Eng. Comput. Sci.* **2022**, *26*, 974. [CrossRef]
271. Babiker Mohamed, M.; Matthew Alofe, O.; Ajmal Azad, M.; Singh Lallie, H.; Fatema, K.; Sharif, T. A Comprehensive Survey on Secure Software-defined Network for the Internet of Things. *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e4391. [CrossRef]
272. Han, D.; Zhu, Y.; Li, D.; Liang, W.; Souri, A.; Li, K.-C. A Blockchain-Based Auditable Access Control System for Private Data in Service-Centric IoT Environments. *IEEE Trans. Ind. Inform.* **2022**, *18*, 3530–3540. [CrossRef]
273. Moustaka, V.; Theodosiou, Z.; Vakali, A.; Kounoudes, A.; Anthopoulos, L.G. Enhancing Social Networking in Smart Cities: Privacy and Security Borderlines. *Technol. Forecast. Soc. Change* **2019**, *142*, 285–300. [CrossRef]
274. Mohanty, S.P.; Kougianos, E.; Guturu, P. SBPG: Secure Better Portable Graphics for Trustworthy Media Communications in the IoT. *IEEE Access* **2018**, *6*, 5939–5953. [CrossRef]
275. Mugarza, I.; Amurrio, A.; Azketa, E.; Jacob, E. Dynamic Software Updates to Enhance Security and Privacy in High Availability Energy Management Applications in Smart Cities. *IEEE Access* **2019**, *7*, 42269–42279. [CrossRef]
276. Safa, N.S.; Mitchell, F.; Maple, C.; Azad, M.A.; Dabbagh, M. Privacy Enhancing Technologies (<scp>PETs</Scp>) for Connected Vehicles in Smart Cities. *Trans. Emerg. Telecommun. Technol.* **2020**, *49*, 715–728. [CrossRef]
277. Yang, W.; Lam, P.T.I. Evaluating Non-Market Costs of ICT Involving Data Transmission in Smart Cities. *Build. Res. Inf.* **2021**, *49*, 715–728. [CrossRef]
278. Wang, Z.; Xu, J.; He, X.; Wang, Y. Analysis of Spatiotemporal Influence Patterns of Toxic Gas Monitoring Concentrations in an Urban Drainage Network Based on IoT and GIS. *Pattern Recognit. Lett.* **2020**, *138*, 237–246. [CrossRef]
279. Wu, F.; Xu, T.; Guo, J.; Huang, B.; Xu, C.; Wang, J.; Li, X. Deep Siamese Cross-Residual Learning for Robust Visual Tracking. *IEEE Internet Things J.* **2021**, *8*, 15216–15227. [CrossRef]
280. Vogiatzaki, M.; Zerefos, S.; Hoque Tania, M. Enhancing City Sustainability through Smart Technologies: A Framework for Automatic Pre-Emptive Action to Promote Safety and Security Using Lighting and ICT-Based Surveillance. *Sustainability* **2020**, *12*, 6142. [CrossRef]
281. Zhang, Y.J.; Alazab, M.; Muthu, B. Machine Learning-Based Holistic Privacy Decentralized Framework for Big Data Security and Privacy in Smart City. *Arab. J. Sci. Eng.* **2021**, *48*, 4141. [CrossRef]

282. Zhang, M.; Wang, X.; Sathishkumar, V.E.; Sivakumar, V. Machine Learning Techniques Based on Security Management in Smart Cities Using Robots. *Work* **2021**, *68*, 891–902. [CrossRef] [PubMed]
283. Lv, Y.; Su, D. Blockchain Security Technology Based on the Asynchronous Transmission Mode of IoT Technology in Smart Cities. *Wirel. Pers. Commun.* **2021**, *126*, 1965–1980. [CrossRef]
284. Chaturvedi, K.; Matheus, A.; Nguyen, S.H.; Kolbe, T.H. Securing Spatial Data Infrastructures for Distributed Smart City Applications and Services. *Futur. Gener. Comput. Syst.* **2019**, *101*, 723–736. [CrossRef]
285. Al-Turjman, F.; Zahmatkesh, H.; Shahroze, R. An Overview of Security and Privacy in Smart Cities' IoT Communications. *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e3677. [CrossRef]
286. Dahmane, W.M.; Ouchani, S.; Bouarfa, H. Towards a Reliable Smart City through Formal Verification and Network Analysis. *Comput. Commun.* **2021**, *180*, 171–187. [CrossRef]
287. Miao, Y.; Ma, J.; Jiang, Q.; Li, X.; Sangaiah, A.K. Verifiable Keyword Search over Encrypted Cloud Data in Smart City. *Comput. Electr. Eng.* **2018**, *65*, 90–101. [CrossRef]
288. Maltezos, E.; Lioupis, P.; Dadoukis, A.; Karagiannidis, L.; Ouzounoglou, E.; Krommyda, M.; Amditis, A.A. Video Analytics System for Person Detection Combined with Edge Computing. *Computation* **2022**, *10*, 35. [CrossRef]
289. Miraftabzadeh, S.A.; Rad, P.; Choo, K.-K.R.; Jamshidi, M. A Privacy-Aware Architecture at the Edge for Autonomous Real-Time Identity Reidentification in Crowds. *IEEE Internet Things J.* **2018**, *5*, 2936–2946. [CrossRef]
290. Gopi, R.; Muthusamy, P.; Suresh, P.G.; Santhosh Kumar, C.G.V.; Pustokhina, I.A.; Pustokhin, D.; Shankar, K. Optimal Confidential Mechanisms in Smart City Healthcare. *Comput. Mater. Contin.* **2022**, *70*, 4883–4896. [CrossRef]
291. Li, X.; Niu, J.; Kumari, S.; Wu, F.; Choo, K.-K.R. A Robust Biometrics Based Three-Factor Authentication Scheme for Global Mobility Networks in Smart City. *Futur. Gener. Comput. Syst.* **2018**, *83*, 607–618. [CrossRef]
292. Sengan, S.; Subramaniyaswamy, V.; Nair, S.K.; Indragandhi, V.; Manikandan, J.; Ravi, L. Enhancing Cyber–Physical Systems with Hybrid Smart City Cyber Security Architecture for Secure Public Data-Smart Network. *Futur. Gener. Comput. Syst.* **2020**, *112*, 724–737. [CrossRef]
293. Tanveer, M.; Khan, A.U.; Alkhayyat, A.; Chaudhry, S.A.; Zikria, Y.B.; Kim, S.W. REAS-TMIS: Resource-Efficient Authentication Scheme for Telecare Medical Information System. *IEEE Access* **2022**, *10*, 23008–23021. [CrossRef]
294. Xu, C.; Lin, H.; Wu, Y.; Guo, X.; Lin, W. An SDNFV-Based DDoS Defense Technology for Smart Cities. *IEEE Access* **2019**, *7*, 137856–137874. [CrossRef]
295. Makkar, A. SecureEngine: Spammer Classification in Cyber Defence for Leveraging Green Computing in Sustainable City. *Sustain. Cities Soc.* **2022**, *79*, 103658. [CrossRef]
296. Rahouti, M.; Xiong, K.; Xin, Y. Secure Software-Defined Networking Communication Systems for Smart Cities: Current Status, Challenges, and Trends. *IEEE Access* **2021**, *9*, 12083–12113. [CrossRef]
297. Sharma, R.; Arya, R. A Secure Authentication Technique for Connecting Different IoT Devices in the Smart City Infrastructure. *Clust. Comput.* **2022**, *25*, 2333–2349. [CrossRef]
298. Shen, J.; Liu, D.; Sun, X.; Wei, F.; Xiang, Y. Efficient Cloud-Aided Verifiable Secret Sharing Scheme with Batch Verification for Smart Cities. *Futur. Gener. Comput. Syst.* **2020**, *109*, 450–456. [CrossRef]
299. Li, D.; Deng, L.; Lee, M.; Wang, H. IoT Data Feature Extraction and Intrusion Detection System for Smart Cities Based on Deep Migration Learning. *Int. J. Inf. Manag.* **2019**, *49*, 533–545. [CrossRef]
300. Li, D.; Deng, L.; Liu, W.; Su, Q. Improving Communication Precision of IoT through Behavior-Based Learning in Smart City Environment. *Futur. Gener. Comput. Syst.* **2020**, *108*, 512–520. [CrossRef]
301. Lim, Y.; Edelenbos, J.; Gianoli, A. Smart Energy Transition: An Evaluation of Cities in South Korea. *Informatics* **2019**, *6*, 50. [CrossRef]
302. Subakti, P.; Putra, Y.H. Integration of TOGAF 9.1 ADM in Enterprise Architecture Smart City Design in the Tourism Domain with ISO 27001. *IOP Conf. Ser. Mater. Sci. Eng.* **2020**, *879*, 12029. [CrossRef]
303. Bawany, N.Z.; Shamsi, J.A. SEAL: SDN Based Secure and Agile Framework for Protecting Smart City Applications from DDoS Attacks. *J. Netw. Comput. Appl.* **2019**, *145*, 102381. [CrossRef]
304. Basmi, W.; Boulmakoul, A.; Karim, L.; Lbath, A. Modern Approach to Design a Distributed and Scalable Platform Architecture for Smart Cities Complex Events Data Collection. *Procedia Comput. Sci.* **2020**, *170*, 43–50. [CrossRef]
305. Chatterjee, S.; Kar, A.K. Effects of Successful Adoption of Information Technology Enabled Services in Proposed Smart Cities of India. *J. Sci. Technol. Policy Manag.* **2018**, *9*, 189–209. [CrossRef]
306. Chmielarz, W.; Zborowski, M.; Fandrejewska, A.; Atasever, M. The Contribution of Socio-Cultural Aspects of Smartphone Applications to Smart City Creation. Poland–Turkey Comparison. *Energies* **2021**, *14*, 2821. [CrossRef]
307. Hassan, S.-U.; Shabbir, M.; Iqbal, S.; Said, A.; Kamiran, F.; Nawaz, R.; Saif, U. Leveraging Deep Learning and SNA Approaches for Smart City Policing in the Developing World. *Int. J. Inf. Manage.* **2021**, *56*, 102045. [CrossRef]
308. Colla, M.; Santos, G.D. Public Safety Decision-Making in the Context of Smart and Sustainable Cities. *Procedia Manuf.* **2019**, *39*, 1937–1945. [CrossRef]
309. Manfreda, A.; Ljubi, K.; Groznik, A. Autonomous Vehicles in the Smart City Era: An Empirical Study of Adoption Factors Important for Millennials. *Int. J. Inf. Manag.* **2021**, *58*, 102050. [CrossRef]

310. Sinaeepourfard, A.; Garcia, J.; Masip-Bruin, X.; Marin-Tordera, E. Data Preservation through Fog-to-Cloud (F2C) Data Management in Smart Cities. In Proceedings of the 2018 IEEE 2nd International Conference on Fog and Edge Computing (ICFEC), Washington, DC, USA, 1–3 May 2018; IEEE: New York, NY, USA, 2018; pp. 1–9.
311. Yandri, E.; Hendroko Setyobudi, R.; Susanto, H.; Abdullah, K.; Adhi Nugroho, Y.; Krido Wahono, S.; Wijayanto, F.; Nurdiansyah, Y. Conceptualizing Indonesia's ICT-Based Energy Security Tracking System with Detailed Indicators from Smart City Extension. *E3S Web Conf.* **2020**, *188*, 7. [CrossRef]
312. Gandhi, B.M.K. A Prototype for IoT Based Car Parking Management System for Smart Cities. *Indian J. Sci. Technol.* **2016**, *9*, 1–6. [CrossRef]
313. Patil, B. Novel NDN Based Routing Protocol for IoT Empowered Savvy City Applications. *J. Adv. Res. Dyn. Control Syst.* **2020**, *12*, 235–243. [CrossRef]
314. Rodriguez-Hernandez, M.A.; Gomez-Sacristan, A.; Gomez-Cuadrado, D. SimulCity: Planning Communications in Smart Cities. *IEEE Access* **2019**, *7*, 46870–46884. [CrossRef]
315. Schleicher, J.M.; Vögler, M.; Inzinger, C.; Dustdar, S. Modeling and Management of Usage-Aware Distributed Datasets for Global Smart City Application Ecosystems. *PeerJ Comput. Sci.* **2017**, *3*, e115. [CrossRef]
316. Yang, Y.-S.; Lee, S.-H.; Chen, G.-S.; Yang, C.-S.; Huang, Y.-M.; Hou, T.-W. An Implementation of High Efficient Smart Street Light Management System for Smart City. *IEEE Access* **2020**, *8*, 38568–38585. [CrossRef]
317. Denker, A. Protection of Privacy and Personal Data in the Big Data Environment of Smart Cities. *Int. Arch. Photogramm. Remote Sens. Spat. Inf. Sci.* **2021**, *46*, 181–186. [CrossRef]
318. Huang, Z.; Peng, Y.; Li, J.; Tong, F.; Zhu, K.; Peng, L. Secrecy Enhancing of SSK Systems for IoT Applications in Smart Cities. *IEEE Internet Things J.* **2021**, *8*, 6385–6392. [CrossRef]
319. Guo, Y.; Zou, K.; Liu, C.; Sun, Y. Study on the Evolutionary Game of Information Security Supervision in Smart Cities under Different Reward and Punishment Mechanisms. *Discret. Dyn. Nat. Soc.* **2022**, *2022*, 8122630. [CrossRef]
320. Gopinath, M.P.; Tamizharasi, G.S.; Kavisankar, L.; Sathyaraj, R.; Karthi, S.; Aarthy, S.L.; Balamurugan, B. A Secure Cloud-Based Solution for Real-Time Monitoring and Management of Internet of Underwater Things (IOUT). *Neural Comput. Appl.* **2019**, *31*, 293–308. [CrossRef]
321. Ali, Z.; Alzahrani, B.A.; Barnawi, A.; Al-Barakati, A.; Vijayakumar, P.; Chaudhry, S.A. TC-PSLAP: Temporal Credential-Based Provably Secure and Lightweight Authentication Protocol for IoT-Enabled Drone Environments. *Secur. Commun. Netw.* **2021**, *2021*, 9919460. [CrossRef]
322. Alam, R.G.G.; Ibrahim, H. Cybersecurity Strategy for Smart City Implementation. *Int. Arch. Photogramm. Remote Sens. Spat. Inf. Sci.* **2019**, *42*, 3–6. [CrossRef]
323. Ayala-Ruiz, D.; Castillo Atoche, A.; Ruiz-Ibarra, E.; Osorio de la Rosa, E.; Vázquez Castillo, J. A Self-Powered PMFC-Based Wireless Sensor Node for Smart City Applications. *Wirel. Commun. Mob. Comput.* **2019**, *2019*, 8986302. [CrossRef]
324. Sharma, S.; Ghanshala, K.K.; Mohan, S. Blockchain-Based Internet of Vehicles (IoV): An Efficient Secure Ad Hoc Vehicular Networking Architecture. In Proceedings of the 2019 IEEE 2nd 5G World Forum (5GWF), Dresden, Germany, 30 October–2 September 2019; IEEE: New York, NY, USA, 2019; pp. 452–457.
325. Pacheco, J.; Benitez, V.H.; Pan, Z. Security Framework for IoT End Nodes with Neural Networks. *Int. J. Mach. Learn. Comput.* **2019**, *9*, 381–386. [CrossRef]
326. Peixoto, J.P.J.; Costa, D.G. Wireless Visual Sensor Networks for Smart City Applications:A Relevance-Based Approach for Multiple Sinks Mobility. *Futur. Gener. Comput. Syst.* **2017**, *76*, 51–62. [CrossRef]
327. Satamraju, K.P.; Malarkodi, B. A Secured and Authenticated Internet of Things Model Using Blockchain Architecture. In Proceedings of the 2019 TEQIP III Sponsored International Conference on Microwave Integrated Circuits, Photonics and Wireless Networks (IMICPW), Tiruchirappalli, India, 22–24 May 2019; IEEE: New York, NY, USA, 2019; pp. 19–23.
328. Puliafito, A.; Tricomi, G.; Zafeiropoulos, A.; Papavassiliou, S. Smart Cities of the Future as Cyber Physical Systems: Challenges and Enabling Technologies. *Sensors* **2021**, *21*, 3349. [CrossRef]
329. Turchet, L.; Fazekas, G.; Lagrange, M.; Ghadikolaei, H.S.; Fischione, C. The Internet of Audio Things: State of the Art, Vision, and Challenges. *IEEE Internet Things J.* **2020**, *7*, 10233–10249. [CrossRef]
330. Gao, W.; Yu, W.; Liang, F.; Hatcher, W.G.; Lu, C. Privacy-Preserving Auction for Big Data Trading Using Homomorphic Encryption. *IEEE Trans. Netw. Sci. Eng.* **2020**, *7*, 776–791. [CrossRef]
331. Hassan, M.; Jincai, C.; Iftekhar, A.; Cui, X. Future of the Internet of Things Emerging with Blockchain and Smart Contracts. *Int. J. Adv. Comput. Sci. Appl.* **2020**, *11*, 631–635. [CrossRef]
332. Dutta, M.; Granjal, J. Towards a Secure Internet of Things: A Comprehensive Study of Second Line Defense Mechanisms. *IEEE Access* **2020**, *8*, 127272–127312. [CrossRef]
333. Jararweh, Y.; Al-Ayyoub, M.; Al-Zoubi, D.; Benkhelifa, E. An Experimental Framework for Future Smart Cities Using Data Fusion and Software Defined Systems: The Case of Environmental Monitoring for Smart Healthcare. *Futur. Gener. Comput. Syst.* **2020**, *107*, 883–897. [CrossRef]
334. Karthick Raghunath, K.M.; Koti, M.S.; Sivakami, R.; Vinoth Kumar, V.; NagaJyothi, G.; Muthukumaran, V. Utilization of IoT-Assisted Computational Strategies in Wireless Sensor Networks for Smart Infrastructure Management. *Int. J. Syst. Assur. Eng. Manag.* **2022**, 1–7. Available online: https://link.springer.com/article/10.1007/s13198-021-01585-y (accessed on 17 October 2023). [CrossRef]

335. NERC. *Annual Report*; NERC: Washington, DC, USA, 2019; Volume 61.
336. Poleto, T.; de Oliveira, R.C.P.; da Silva, A.L.B.; de Carvalho, V.D.H. Using Fuzzy Cognitive Map Approach for Assessing Cybersecurity for Telehealth Scenario. In *Trends and Innovations in Information Systems and Technologies*; Rocha, Á., Adeli, H., Reis, L.P., Costanzo, S., Orovic, I., Moreira, F., Eds.; Springer: Cham, Switzerland, 2020; pp. 828–837.
337. Rahim, N.H.A.; Hamid, S.; Kiah, L.M.; Shamshirband, S.; Furnell, S. A Systematic Review of Approaches to Assessing Cybersecurity Awareness. *Kybernetes* **2015**, *44*, 606–622. [CrossRef]
338. Hao, S.; Wang, W.; Yan, Y.; Bruzzone, L. Class-Wise Dictionary Learning for Hyperspectral Image Classification. *Neurocomputing* **2017**, *220*, 121–129. [CrossRef]
339. Molzahn, D.K.; Wang, J. Detection and Characterization of Intrusions to Network Parameter Data in Electric Power Systems. *IEEE Trans. Smart Grid* **2019**, *10*, 3919–3928. [CrossRef]
340. Kott, A.; Alberts, D.S.; Wang, C. Will Cybersecurity Dictate the Outcome of Future Wars. *Computer* **2015**, *48*, 98–101. [CrossRef]
341. Wang, X.; Luo, H.; Qin, X.; Feng, J.; Gao, H.; Feng, Q. Evaluation of Performance and Impacts of Maternal and Child Health Hospital Services Using Data Envelopment Analysis in Guangxi Zhuang Autonomous Region, China: A Comparison Study among Poverty and Non-Poverty County Level Hospitals. *Int. J. Equity Health* **2016**, *15*, 131. [CrossRef]
342. Liu, M.; Li, K.; Chen, T. Security Testing of Web Applications: A Search-Based Approach for Detecting SQL Injection Vulnerabilities. In Proceedings of the 2019 Genetic and Evolutionary Computation Conference Companion, Prague, Czech Republic, 13–17 July 2019; pp. 417–418.
343. Liu, M.; Li, K.; Chen, T. Security Testing of Web Applications. In Proceedings of the Genetic and Evolutionary Computation Conference Companion on–GECCO '19, Prague, Czech Republic, 13–17 July 2019; ACM Press: New York, NY, USA, 2019; pp. 417–418.
344. Liu, N.; Zhang, J.; Liu, W. A Security Mechanism of Web Services-Based Communication for Wind Power Plants. *IEEE Trans. Power Deliv.* **2008**, *23*, 1930–1938. [CrossRef]
345. Feng, N.; Wang, H.J.; Li, M. A Security Risk Analysis Model for Information Systems: Causal Relationships of Risk Factors and Vulnerability Propagation Analysis. *Inf. Sci.* **2014**, *256*, 57–73. [CrossRef]
346. Farley, R.; Wang, X. Exploiting VoIP Softphone Vulnerabilities to Disable Host Computers: Attacks and Mitigation. *Int. J. Crit. Infrastruct. Prot.* **2014**, *7*, 141–154. [CrossRef]
347. Ten, C.W.; Liu, C.C.; Manimaran, G. Vulnerability Assessment of Cybersecurity for SCADA Systems. *IEEE Trans. Power Syst.* **2008**, *23*, 1836–1846. [CrossRef]
348. Fournaris, A.P.; Fraile, L.P.; Koufopavlou, O. Exploiting Hardware Vulnerabilities to Attack Embedded System Devices: A Survey of Potent Microarchitectural Attacks. *Electronics* **2017**, *6*, 52. [CrossRef]
349. Kao, D.Y.; Wang, S.J.; Fu-Yuan Huang, F. SoTE: Strategy of Triple-E on Solving Trojan Defense in Cyber-Crime Cases. *Comput. Law Secur. Rev.* **2010**, *26*, 52–60. [CrossRef]
350. Mimo, E.M.; McDaniel, T. 3D Privacy Framework: The Citizen Value Driven Privacy Framework. In Proceedings of the 2021 IEEE International Smart Cities Conference (ISC2), Paphos, Cyprus, 7–10 September 2021; IEEE: New York, NY, USA, 2021; pp. 1–7.
351. Hu, G.; Xiao, D.; Xiang, T.; Bai, S.; Zhang, Y. A Compressive Sensing Based Privacy Preserving Outsourcing of Image Storage and Identity Authentication Service in Cloud. *Inf. Sci.* **2017**, *387*, 132–145. [CrossRef]
352. Foroutan, S.A.; Salmasi, F.R. Detection of False Data Injection Attacks against State Estimation in Smart Grids Based on a Mixture Gaussian Distribution Learning Method. *IET Cyber Phys. Syst. Theory Appl.* **2017**, *2*, 161–171. [CrossRef]
353. Alami, H.; Gagnon, M.-P.; Ag Ahmed, M.A.; Fortin, J.-P. Digital Health: Cybersecurity Is a Value Creation Lever, Not Only a Source of Expenditure. *Heal. Policy Technol.* **2019**, *8*, 319–321. [CrossRef]
354. Paul, J.A.; Wang, X. (Jocelyn) Socially Optimal IT Investment for Cybersecurity. *Decis. Support Syst.* **2019**, *122*, 113069. [CrossRef]
355. Enoch, S.Y.; Ge, M.; Hong, J.B.; Alzaid, H.; Kim, D.S. A Systematic Evaluation of Cybersecurity Metrics for Dynamic Networks. *Comput. Netw.* **2018**, *144*, 216–229. [CrossRef]
356. Zhang, J.; Dong, Q. Efficient ID-Based Public Auditing for the Outsourced Data in Cloud Storage. *Inf. Sci.* **2016**, *343–344*, 1–14. [CrossRef]
357. Xin, Y.; Kong, L.; Liu, Z.; Chen, Y.; Li, Y.; Zhu, H.; Gao, M.; Hou, H.; Wang, C. Machine Learning and Deep Learning Methods for Cybersecurity. *IEEE Access* **2018**, *6*, 35365–35381. [CrossRef]
358. Montesdioca, G.P.Z.; Maçada, A.C.G. Measuring User Satisfaction with Information Security Practices. *Comput. Secur.* **2015**, *48*, 267–280. [CrossRef]
359. Ten, C.W.; Ginter, A.; Bulbul, R. Cyber-Based Contingency Analysis. *IEEE Trans. Power Syst.* **2016**, *31*, 3040–3050. [CrossRef]
360. Hong, J.; Liu, C.C.; Govindarasu, M. Integrated Anomaly Detection for Cyber Security of the Substations. *IEEE Trans. Smart Grid* **2014**, *5*, 1643–1653. [CrossRef]
361. Hong, J.; Nuqui, R.F.; Kondabathini, A.; Ishchenko, D.; Martin, A. Cyber Attack Resilient Distance Protection and Circuit Breaker Control for Digital Substations. *IEEE Trans. Ind. Inform.* **2019**, *15*, 4332–4341. [CrossRef]
362. Sterlini, P.; Massacci, F.; Kadenko, N.; Fiebig, T.; Van Eeten, M. Governance Challenges for European Cybersecurity Policies: Stakeholder Views. *IEEE Secur. Priv.* **2020**, *18*, 46–54. [CrossRef]
363. Charlet, K.; King, H. The Future of Cybersecurity Policy. *IEEE Secur. Priv.* **2020**, *18*, 8–10. [CrossRef]

364. Vattapparamban, E.; Güvenç, I.; Yurekli, A.I.; Akkaya, K.; Uluağaç, S. Drones for Smart Cities: Issues in Cybersecurity, Privacy, and Public Safety. In Proceedings of the International Wireless Communications and Mobile Computing Conference, IWCMC, Paphos, Cyprus, 5–9 September 2016; pp. 216–221. [CrossRef]
365. Khatoun, R.; Zeadally, S. Cybersecurity and Privacy Solutions in Smart Cities. *IEEE Commun. Mag.* **2017**, *55*, 51–59. [CrossRef]
366. Zimmermann, V.; Renaud, K. Moving from a "human-as-Problem" to a "human-as-Solution" Cybersecurity Mindset. *Int. J. Hum. Comput. Stud.* **2019**, *131*, 169–187. [CrossRef]
367. Woods, D.W.; Moore, T. Does Insurance Have a Future in Governing Cybersecurity? *IEEE Secur. Priv.* **2020**, *18*, 21–27. [CrossRef]
368. Maddux, J.E.; Rogers, R.W. Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change. *J. Exp. Soc. Psychol.* **1983**, *19*, 469–479. [CrossRef]
369. Biswas, K.; Muthukkumarasamy, V. Securing Smart Cities Using Blockchain Technology. In Proceedings of the 2016 IEEE 18th International Conference on High Performance Computing and Communications, IEEE 14th International Conference on Smart City, IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Sydney, Australia, 12–14 December 2016; IEEE: New York, NY, USA, 2016; pp. 1392–1393.
370. Zhang, K.; Ni, J.; Yang, K.; Liang, X.; Ren, J.; Shen, X.S. Security and Privacy in Smart City Applications: Challenges and Solutions. *IEEE Commun. Mag.* **2017**, *55*, 122–129. [CrossRef]
371. Sivanathan, A.; Gharakheili, H.H.; Loi, F.; Radford, A.; Wijenayake, C.; Vishwanath, A.; Sivaraman, V. Classifying IoT Devices in Smart Environments Using Network Traffic Characteristics. *IEEE Trans. Mob. Comput.* **2019**, *18*, 1745–1759. [CrossRef]
372. Sharma, P.K.; Moon, S.Y.; Park, J.H. Block-VN: A Distributed Blockchain Based Vehicular Network Architecture in Smart City. *J. Inf. Process. Syst.* **2017**, *13*, 184–195. [CrossRef]
373. Khatoun, R.; Zeadally, S. Smart Cities: Concepts, Architectures, Research Opportunities. *Commun. ACM* **2016**, *59*, 46–57. [CrossRef]
374. Djahel, S.; Doolan, R.; Muntean, G.-M.; Murphy, J. A Communications-Oriented Perspective on Traffic Management Systems for Smart Cities: Challenges and Innovative Approaches. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 125–151. [CrossRef]
375. Sharma, P.K.; Park, J.H. Blockchain Based Hybrid Network Architecture for the Smart City. *Futur. Gener. Comput. Syst.* **2018**, *86*, 650–655. [CrossRef]
376. Angelidou, M. The Role of Smart City Characteristics in the Plans of Fifteen Cities. *J. Urban Technol.* **2017**, *24*, 3–28. [CrossRef]
377. Rathore, M.M.; Paul, A.; Hong, W.-H.; Seo, H.; Awan, I.; Saeed, S. Exploiting IoT and Big Data Analytics: Defining Smart Digital City Using Real-Time Urban Data. *Sustain. Cities Soc.* **2018**, *40*, 600–610. [CrossRef]
378. Qiu, T.; Chen, N.; Li, K.; Qiao, D.; Fu, Z. Heterogeneous Ad Hoc Networks: Architectures, Advances and Challenges. *Ad Hoc Netw.* **2017**, *55*, 143–152. [CrossRef]
379. Petit, J.; Shladover, S.E. Potential Cyberattacks on Automated Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2015**, *16*, 546–556. [CrossRef]
380. Nepomuceno, T.C.C.; Silva, W.M.N.; Nepomuceno, K.T.C.; Barros, I.K.F. A DEA-Based Complexity of Needs Approach for Hospital Beds Evacuationduring the COVID-19 Outbreak. *J. Healthc. Eng.* **2020**, *2020*, 8857553. [CrossRef]
381. Daraio, C.; Kerstens, K.; Nepomuceno, T.; Sickles, R.C. Empirical Surveys of Frontier Applications: A Meta-Review. *Int. Trans. Oper. Res.* **2020**, *27*, 709–738. [CrossRef]
382. Watzlaf, V.J.M.; Zhou, L.; DeAlmeida, D.R.; Hartman, L.M. A Systematic Review of Research Studies Examining Telehealth Privacy and Security Practices Used By Healthcare Providers. *Int. J. Telerehabil.* **2017**, *9*, 39–58. [CrossRef]
383. Schukat, M. Securing Critical Infrastructure. In Proceedings of the 10th International Conference on Digital Technologies, Zilina, Slovakia, 9–11 July 2014; pp. 298–304.
384. Zhu, K.; Ying, S.; Ding, W.; Zhang, N.; Zhu, D. IVKMP: A Robust Data-Driven Heterogeneous Defect Model Based on Deep Representation Optimization Learning. *Inf. Sci.* **2022**, *583*, 332–363. [CrossRef]
385. Ferraz, F.S.; Guimaraes Ferraz, C.A. More than Meets the Eye in Smart City Information Security: Exploring Security Issues Far beyond Privacy Concerns. In Proceedings of the 2014 IEEE 11th International Conference on Ubiquitous Intelligence and Computing and 2014 IEEE 11th International Conference on Autonomic and Trusted Computing and 2014 IEEE 14th International Conference on Scalable Computing and Communications and Its Associated Workshops, Bali, Indonesia, 9–12 December 2014; IEEE: New York, NY, USA, 2014; pp. 677–685.
386. Zheng, K.; Albert, L.A.; Luedtke, J.R.; Towle, E. A Budgeted Maximum Multiple Coverage Model for Cybersecurity Planning and Management. *IISE Trans.* **2019**, *51*, 1303–1317. [CrossRef]
387. Santos, J.R.; Haimes, Y.Y.; Lian, C. A Framework for Linking Cybersecurity Metrics to the Modeling of Macroeconomic Interdependencies. *Risk Anal.* **2007**, *27*, 1283–1297. [CrossRef] [PubMed]
388. Bergström, E.; Lundgren, M.; Ericson, Å. Revisiting Information Security Risk Management Challenges: A Practice Perspective. *Inf. Comput. Secur.* **2019**, *27*, 358–372. [CrossRef]
389. Daraio, C.; Kerstens, K.H.J.; Nepomuceno, T.C.C.; Sickles, R. Productivity and Efficiency Analysis Software: An Exploratory Bibliographical Survey of the Options. *J. Econ. Surv.* **2019**, *33*, 85–100. [CrossRef]