sustainability

MDPI

Article

Conceptual Model of Key Aspects of Security and Privacy Protection in a Smart City in Slovakia

Michaela Kollarova [1,2], Tomas Granak [2], Stanislava Strelcova [1] and Jozef Ristvej [1,*]

[1] Department of Crisis Management, Faculty of Security Engineering, University of Žilina, Univerzitná 1, 010 26 Žilina, Slovakia; michaela.kollarova@mod.gov.sk (M.K.); stanislava.strelcova@uniza.sk (S.S.)
[2] Ministry of Defence of the Slovak Republic, Kutuzovova 8, 832 47 Bratislava, Slovakia; tomas.granak@mod.gov.sk
* Correspondence: jozef.ristvej@uniza.sk; Tel.: +421-41-513-5130

Abstract: The output of this work is a comprehensive overview of a wide range of key aspects of security and privacy relevant for the development of smart cities in Slovakia. The work incorporates heterogeneous and complex findings into a corpus of simplified evidence. By employing a systematic review method, this study first outlines key characteristics of a smart city, and then proceeds to summarise opportunities and challenges for conceptualising a model of a smart city in Slovakia. The development of a classification with respect to the different smart city domains, systems and potential threats aims to highlight universally applicable aspects. In order to provide an overview, the paper also presents specific requirements, options, problems, and factors taking into account Slovak policies. This work is based on the proposition that a sustainable and prosperous conceptual model of a smart city is not only linked with technological artefacts and communication infrastructure that enable intelligent management of various governance resources, but is especially tied to the norms, policies, and standards that ensure security and privacy for smart city residents, as their presence and trust in the whole ecosystem is essential for the generation, collection, processing, storage, dissemination, and use of data by respectful technologies. A secure smart city is a cross-disciplinary dilemma, a universal technological challenge built upon context-based policies, standards and procedures. The output of this work is an identification of smart city domains that can become subject to attacks and a stipulation of security requirements that are needed to assure domain functionality. Maintaining meaningful human control as a requirement to mitigate influence activities as well as protect and ensure residential engagement in a smart city was identified and added to the results of the review. Simple communication was highlighted as an effective countermeasure. Applicability of the smart city concept in Slovakia is particularly vulnerable due to the slow pace of implementation and fragmentation of relevant legislation, short development cycle of new techniques of attack, and the lack of expertise and low level of user awareness.

Keywords: security; privacy; protection; smart city; sustainability

check for updates

Citation: Kollarova, M.; Granak, T.; Strelcova, S.; Ristvej, J. Conceptual Model of Key Aspects of Security and Privacy Protection in a Smart City in Slovakia. *Sustainability* **2023**, *15*, 6926. https://doi.org/10.3390/su15086926

Academic Editors: Dezhi Li, Mohamed A. Mohamed, Chao Mao and Shenghua Zhou

Received: 5 January 2023
Revised: 14 April 2023
Accepted: 17 April 2023
Published: 20 April 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

A smart city is a space that integrates physical, digital, and societal systems into networks and services to better leverage available resources, improve interaction with government as well as improve the well-being of its residents [1,2]. A more comprehensive definition frames a smart city as an urban space that uses existing physical infrastructure and various technologies such as the Internet of Things, physical networks, cyber networks, sensor networks, information and communication technologies as well as intelligence to collect data in different urban areas, and through its rigorous analysis provides a better housing environment and continuously improves the quality of life, economic and social development and growth, promotes sustainable development and environmental protection, makes optimal use of energy resources, improves the performance of urban

systems, solves local problems, and assists in better planning [3–5]. The definition of a smart city goes beyond the use of mechanical or digital technologies, as it also includes political commitment, social investment as well as broad and inclusive engagement of residents, which is essential in delivering sustainable and inclusive solutions that make cities safer and more resilient [6,7]. Developing the smart city concept through the implementation of systemic solutions ranging from cybersecurity policies to responsible data management standards has the potential to exponentially improve the quality of life and trust of smart city inhabitants [8]. In addition to the vast number of benefits that a smart city concept offers, the broader range of challenges and potential risks that their realisation poses for governments, institutions, organisations, and potential service providers need to be addressed and analysed.

In order to provide more value to its residents than conventional cities, smart cities aim to utilise a combination of sensors, software solutions, user interfaces and communication networks, in other words, the Internet of Things (IoT) [9]. IoT has the greatest impact on smart city routine operations and service delivery [10]. It is due to the fact that service delivery and optimisation at an operational level relies heavily on analysing large amounts of data [11]. Citizens and their willingness to engage in the smart city ecosystem therefore plays a critical role. The more citizens and devices are involved in the ecosystem, the greater the amount of data are consciously or unconsciously generated at each point in time, the processing of which can lead to the discovery of behavioural patterns, lifestyle patterns, interests, and consumption habits [12,13]. The safe and lawful generation, collection, transmission, processing, storage, dissemination, and use of data within the smart city ecosystem is the biggest challenge for a sustainable smart city concept implementation [14].

Sustainable digital innovation is linked with the development of digital protection mechanisms [15]. Threats to the security of smart city residents, in the form of data misuse or other breaches of their digital privacy, can lead not only to distrust towards the provided services, but even to a pessimistic perception of the smart city concept. Public policy therefore takes centre stage in determining the extent and fidelity of information that residents of smart cities are willing to contribute [16]. As long as a resident's private data recorded by various sensors and digital solutions are secure, the engagement rate should remain high. On the contrary, if residents do not have the will to actively participate in the IoT ecosystem, the smart city concept will not be able to provide services of a higher quality than a conventional city and will therefore lose its relevance. Quantification of residential engagement through digital means in the Slovak Republic is a trending paradigm, unfortunately, as of now, dominated mainly by private entities, which are collecting data for marketing or system management purposes [16,17]. Slovak policies pertinent to the deployment of information systems in public administration are uncoordinated and fragmented [16]. Consequences of various regional administration agendas include difficulties in combining policy aspects with technological solutions [18]. Based on an overview of smart city systems and major privacy and security issues, the study adds to the existing body of literature by discussing a range of specific solutions for Slovakia to address critical security and privacy threats in smart city infrastructures. Open research issues and challenges are taken into account. A possible system of a smart city is shown on Figure 1.

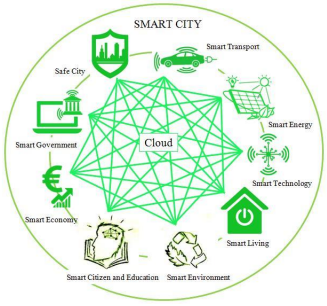

Figure 1. System of a Smart City [19].

1.1. Research Questions

Given the issues presented in the introduction and the identification of a literature gap, this work seeks to answer the following research questions:

1. What are the general security and privacy aspects of a smart city and how can we categorise them?
2. Which of these aspects are critical for the development of a conceptual model of security and privacy in a smart city with respect to the possibilities, assumptions, problems, and factors of its feasibility in the Slovak Republic?

1.2. Literature Review

The smart city was outlined in the introduction and therefore the literature review is dedicated to the specific systems and domains that comprise a smart city. This part describes them on two levels. In the first paragraph, the nine main systems that constitute a smart city and are subject to security and privacy concerns are described based on the Slovak policies and researched literature. Beyond the findings derived from literature research, sustainable finance was added as a designated system as it plays a crucial role in the developing smart city ecosystem in Slovakia. Subsequently, the second paragraph describes a smart city in terms of the general requirements for the aforementioned systems and their security parameters. The study draws inspiration from defence and security research on complex systems and adds meaningful human control as one key requirement. The decision to include this unusual aspect was taken to highlight the importance of linking the security and privacy architecture with the will of residents to be active participants. Given the interconnectedness of all aspects of the smart city and the presence of IoT as a fundamental building block for the entire ecosystem, it is necessary to view security not only through the prism of the systems but also cross-sectionally through the requirements for their functionality.

There are several published papers that systematically review security and privacy aspects of smart cities. Some use case studies to highlight potential security outcomes of developmental programs pursued by smart city administration [20], while others have broader focus and examine contemporary security solutions as a means of addressing general smart city challenges [21]. Research focusing on assessing technologies as key enablers behind security techniques [22] or examining novel applications of IoT systems and discussing their potential implications are also prevalent [23]. Smart city security focused literature tends to discuss various modes of privacy and categorise vectors of possible attacks as well as defence options [24].

1. Smart City Governance: This system primarily relates to municipal politics and citizen participation in public decision-making, management of municipal enterprises, and general services for smart city residents [25]. For instance, digitalisation of local elections, public consultations, referendums, voting, monitoring of residents' sentiment about public affairs or local policies, and others [26]. In the Slovak Republic, municipalities are constitutionally obliged to appropriately inform residents about their activities. Without more detailed elaboration of the means, this obligation is further specified in Act No. 211/2000 Coll. on free access to information.
2. Smart Residents: The system mainly relates to the level of competence and education of residents in the use of technological artefacts and participation in the smart city ecosystem, but also to the ability of residents to actively perceive social interactions and public life and react to emerging changes [27]. Responsible residents who know how to securely handle and share their data are a good example. The principal methods of residential participation in Slovak municipal governance are specified in the Act on the Municipal System no. 369/1990 Coll. The voluntary contribution relies on the municipality's independent initiative [27]. A national programme for development of education as well as a programme of school informatisation with an outlook until 2030 seek to increase competence of the society in the field of ICT and digital services.

3. Smart Economy: This system is mainly linked with competition, entrepreneurship, continuous innovation cycle, flexibility, and labour market productivity [28]. The focus is on how technology is applied rather than how many technological artefacts are available [29]. Examples include special industrial zones or the circular economy. The Smart Industry Concept for Slovakia defines the vision and some domains of a smart economy, while a follow-up action plan is limited to the framing of general tasks that would enable favourable conditions for the development of the Slovak IoT-based economy. The Research and Innovation Strategy for Intelligent Specialisation Slovak Republic 2021–2027 increases the potential for such transformation.
4. Smart Housing: The system encompasses a number of intelligent services designed to improve general quality of life or provide convenient home better management of home appliances [30]. These range from optimisation of residential zones, cultural and social facilities, educational facilities, tourism, and security to remote monitoring [31,32].
5. Smart Healthcare: A connected, intelligent, and human-centred healthcare system is best represented by the integration of personal, environment, and infrastructure data via algorithms to create actionable insights or personalised care experience for smart city residents [33]. Digitalisation and informatisation of the Slovak healthcare system was enabled by Act No. 53/2013 Coll. on the national health information system, which established the National Centre for Health Information responsible for the implementation of informatisation and computerisation of healthcare in the Slovak Republic [34]. This paradigm was further accelerated by the COVID-19 pandemic.
6. Smart Transportation: This system is primarily tied to a sustainable transportation system and the continuous improvement of urban transport efficiency, smart parking, and traffic management in relation to planning and demographic trends [35]. A suitable example are the smart interfaces for public transportation. Act No. 317/2012 Coll. on Intelligent Transport Systems in Road Transport regulates the use of smart transport systems in Slovakia for road transport only. Data collection and analysing are somewhat decentralised and take place at several levels, e.g., the Slovak Road Administration through the National Traffic Information System [36]. This strategy for smart and sustainable mobility in Slovakia provides a vision for the future direction of this system.
7. Smart Infrastructure: This system relates to the monitoring of urban environments and management of limited resources, raw materials, and energy networks in order to ensure their optimal usage [37]. Some examples are smart grid, electricity storage or decentralisation of energy production, and consumption [38]. Providing access to information and communication networks and technologies also falls into this category. The topic of smart energy is one of the priorities of the Energy Union and according to the Ministry of Economy, Slovakia is significantly lagging behind. Act No. 251/2012 Coll. on Energy does not take into account the dynamically changing environment and contemporary trends such as decentralisation [39].
8. Smart Urban Environment: This system comprises monitoring of key ecological indexes and their analyses to adequate responses from authorities. It is an essential link between city management and environmental protection [40]. Examples include, but are not limited to, carbon and harmful gas management, construction of green spaces and buildings, waste recycling, and sanitation management. The vague vision is conveyed by the Strategy of Environmental Policy of the Slovak Republic to 2030. Act No. 17/1992 Coll. on the Environment as well as the forthcoming Act No. 27/2022 Coll. on Air Protection defines sufficient environmental parameters, but there is a lack of legislation framing the means of achieving the desired state.
9. Sustainable Finance: The Slovak Government approved the Programme Slovakia 2021–2027, on the basis of which the Slovak Republic will be able to draw European resources in the amount of almost EUR 13 billion in the new programming period. The package also includes EUR 106.3 million allocated for the building of smart cities and regions, in accordance with the Programme Declaration of the Slovak Government and

other relevant focus materials, including the upcoming Action Plan for Smart Cities and Regions for 2023–2025. The National Investment Plan for 2018–2030 elaborates on the current funding basis and specifies financial instruments at the national level.

According to studies [19,37], structure and relations between the concepts of smart city and safe city, their common systems, and separate layers are shown in Figure 2.

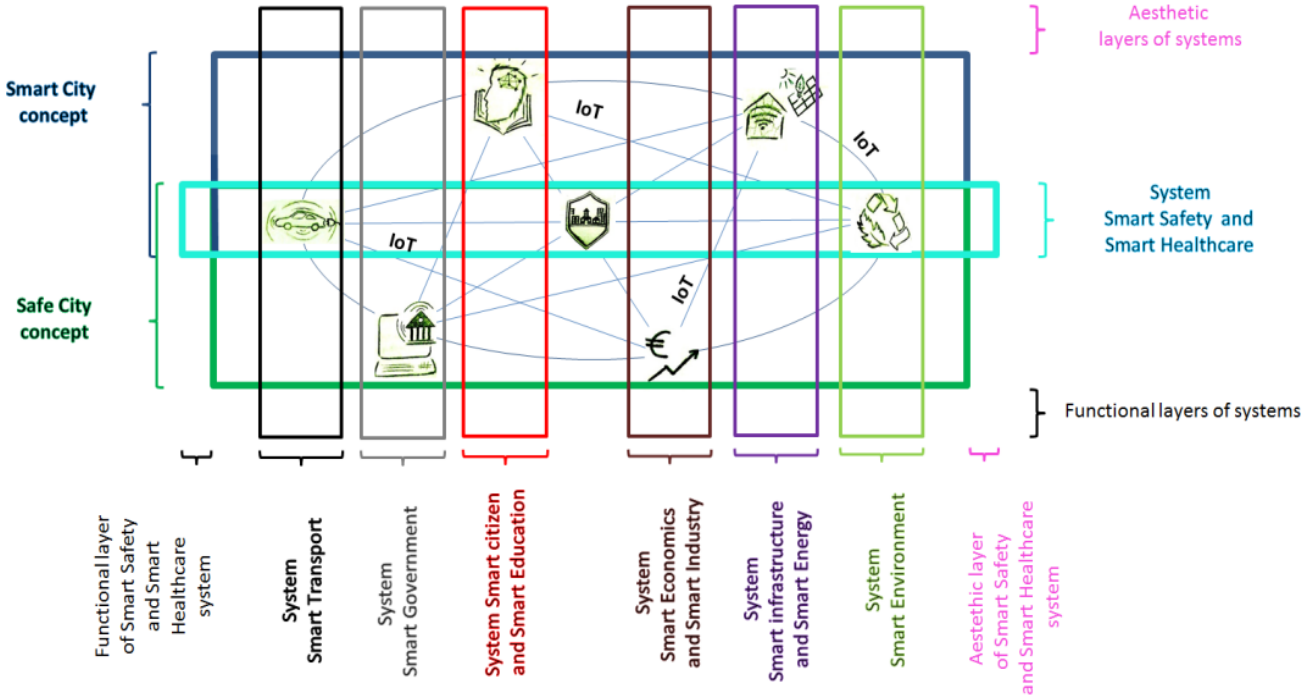

Figure 2. Structure and relations between the concepts of Smart City and Safe City, their common systems, and separate layers [37].

The Act No. 69/2018 on Cybersecurity defines a cybersecurity incident as any event that results in the loss of confidentiality of data, destruction or compromise of system integrity, limitation or denial of availability of an essential or digital service, a high likelihood of compromise of the operations of an essential or digital service, or a compromise of the security of information [41]. While the above-mentioned definition could be applied to all relevant systems of a smart city, to build a conceptual model, it is beneficial to theorise beyond the scope of threats and examine security and privacy protection requirements.

A. An active participation of residents is the backbone of a smart city because the concept itself is based on the premise that technology serves the needs of residents and a smart city is not merely about advanced technology and infrastructure. The participation of residents and their devices is essential due to their ability to generate data for the development of technologies, applications and systems as well as human factors such as innovation [13].
B. Meaningful human control of systems and subsystems. Given the ubiquity of systems in a smart city, it is necessary to take into consideration ethical implications and user values to ensure their socio-technical resilience [42]. Meaningful human control as part of the design ensures sustainable engagement of residents.
C. Onnectivity enables the connection of technological artefacts and their clusters to the intelligent ecosystem represented by IoT [43]. Thus, connectivity is the most fundamental prerequisite for a technically functioning smart city and a guarantor of competitive advantage over conventional cities. Connectivity, through the provision of communication solutions, causes a significant spillover effect to other domains.

D. Scalability complements connectivity, as each IoT system or component should be scalable according to the needs of a smart city. Assuming that smart cities evolve from small to larger, from technologically simpler to more complex, an exponential increase in system complexity as well as data quantity can be expected [44]. A smart city cannot function properly without scalable systems and mechanisms. Connectivity and scalability are directly related to the generation and management of big data (Big Data).
E. Big Data are the result of the application of IoT. As outlined in the introduction, for the operation of a smart city, it is necessary to manage large amounts of sensitive and personal information that may pose a security risk or a vulnerable part of the system.
F. Heterogeneity is another requirement that is related to IoT. Heterogeneity can be defined as the plurality and independence of systems, technological artefacts, users, diversity of networks, protocols and communication technologies, tools, and platforms that lack a common security framework [45]. Homogeneity is in direct conflict with the dynamic concept of the evolving smart city.
G. Constrained resources, or in other words, devices that are a part of IoT are limited by physical parameters such as memory, battery capacity and quality, radio standards or network interfaces [46]. For better security, it is necessary to balance the use of cheaper, smaller, and less energy-intensive devices with their expensive counterparts. Data minimisation and avoiding recording of irrelevant data are also part of effective resource management [47]. Unique security challenges require specific security measures.
H. Autonomy provides rapid response, cost savings, and adaptive configuration of systems as they operate. Autonomy is closely linked to the artificial intelligence (AI) that enables it. Devices involved in IoT, unlike traditional technological artefacts, should be able to configure themselves automatically.
I. Vulnerability or susceptibility of complex systems to coordinated physical attacks and natural disasters is the Achilles heel of IoT [48]. Due to their number, sensors are usually small and do not have robust physical protection. This means that they can be easily destroyed, stolen, moved, or tampered with.

1.3. Literature Gap

The smart city is a trending topic, which is being studied mainly in terms of particular technologies, systems, and policies [49]. This means that a large body of literature focuses on technical ways to increase well-being and improve quality of life or researching enabling policies [50]. Challenges including security and privacy of interconnected domains occupy a disproportionately smaller portion of the literature [51]. Considering the fact that the smart city is a dynamic and evolving topic, there is a demand for cross-disciplinary efforts to cover the diverging literature and identify, classify, and reference critical aspects as well as security requirements with regard to specific scenarios [52]. Numerous types of comprehensive studies have been conducted in the past in this area [53], but one of the missed opportunities is lack of a holistic approach; that is, the various smart city aspects have not been considered in an integrated manner on a concrete example. This work seeks to add to this area in the literature, and additionally link sustainable development with the need to appropriately address the security of smart city residents. The work also fills a gap in the efforts leading to the development of smart city conceptual models [54]. To address these challenges on a practical level, the work first outlines a framework comprising the most important smart city systems and their security and privacy requirements through a systematic review, and then proceeds to consider which of these aspects are critical for the development of a conceptual model of security and privacy in a smart city with respect to the context of the Slovak Republic. The above-mentioned gap is further exacerbated in Slovak literature, which lacks robust literature on categorisation or classification of the problem, but provides room for developing a variety of conceptual models.

2. Materials and Methods

This work utilises a mixed research method primarily based on the method of qualitative systematic review. The method was chosen because it enables effective identification, evaluation, and synthesis of the largest possible set of heterogeneous research relevant to answering the posed research questions [55,56]. This work firstly systematically evaluates a broad scope of smart city systems present in the wider literature, and based on a correlation with systems recognised by Slovak strategic and conceptual policy documents, identifies the nine most important systems. Secondly, requirements relevant to the conceptualisation of the model for smart city security and privacy are stipulated. Thirdly, in a holistic manner, the work proceeds from broad to concrete, considering the possibilities, assumptions, challenges, and feasibility factors for smart city realisation in the Slovak Republic, particularly considering the cyber domain as it is the most prolific. The work results in a systematic synthesis of evidence and elaboration of results according to specific security and privacy domains, based on the synthesis and interpretation of data from a wide range of heterogeneous studies across multiple research domains. It should be noted that due to the high set of relevant systems and domains of security and privacy, the thesis only highlights the most relevant and focuses purely on the conceptual level. Refining and implementing the model itself as well as evaluating the interactions between the different domains is not in the scope of this work. The elaboration of the specific model and evaluating its potential implementation in the Slovak context is the subject of a potential follow-up study. Strategic and conceptual policy documents are not linked to the overarching body of European legislation or normative documents from intergovernmental authorities.

The work uses a comprehensive search strategy using several scientific databases and examines articles published in Slovak, Czech, and English. The search of heterogeneous sources allowed for the analysis and synthesis of a sufficient number of articles, which minimises bias and makes it easier to conduct a systematic review. The systematic review method uses explicit and transparent processes, which are easily reproducible by other parties [57]. The downside of the chosen method is that systematic review is significantly limited by the formulation of the research questions [58]. In practice, this means that the ability of this method to answer unexpected questions or contribute to the wider debate is limited [59]. Another downside of the selected method is selection bias, because research questions are tied to the specific context of the Slovak Republic, but drawn from broad literature [60].

Summary of the Research Process

1. Define the research questions as well as inclusion and exclusion criteria for various privacy and security aspects.
2. Search for relevant academic articles in electronic databases such as JSTOR, ScienceDirect, Scopus, EBSCO, ProQuest.
3. Select highly cited articles with respect to the defined research method, criteria, and timeliness.
4. Filter research articles by title, keywords, and abstract with respect to various aspects of smart city security and privacy.
5. Evaluate bias and extract relevant data from the articles.
6. Analyse and classify key aspects.
7. Reduce and extract key aspects.
8. Categorise key aspects.
9. Assess the quality of evidence and interpretation of categories to achieve a more comprehensive view.
10. Draw generalised conclusions to the aspects beyond their individual elements.
11. Address retrieved conclusions that differ from the literature review and unpack in the discussion.

3. Results

The results present a structured description of the most important aspects related to the conceptual model of smart security and privacy. The selection of aspects takes into account current and future developments in the studied area. The aspects are further incorporated and divided into specific domains, which are intended to simplify the heterogeneous and complex findings regarding the possibilities, assumptions, problems, and feasibility factors of the concept.

3.1. Security

The ubiquity of sensors, networks, and computing technology in urban infrastructure presents different vectors for potential attacks or other malicious activities. Since all of the relevant layers are integrated, in a smart city, any successful breach of privacy and security can lead to an exponentially worsened outcome. General security threats to smart city infrastructure include eavesdropping, theft, denial of service, information tracking, loss of user data, user identity forgery, data content forgery, tampering, data leakage, and botnet activities that target user privacy [61,62]. Hardware threats include tampering with communication nodes, wireless interferences, insertion of malicious nodes or code as well as physical damage. Assuming that the malicious actor is in physical proximity to the devices, attacks may also include destruction of the communication node or radio frequency jamming [63]. Cyber threats include phishing attacks, viruses, worms, and spyware. A separate category is the wide range of hacking attacks that attempt to use malware to gain unauthorised access to network system components [64]. Other network attacks mainly include traffic analysis attacks, unauthorised access, and simulation attacks. Devices with limited computing resources are particularly susceptible to attacks. As was mentioned in the introduction, residential trust in the whole ecosystem is essential. Therefore, a smart city must be explainable to its users, who, under ideal conditions, shall interact with it effortlessly through adequate interfaces. This includes the ability to verify or audit automated processes. Furthermore, one of possible vectors of attack on smart city security is to avoid technological artefacts altogether and erode the trust and will of its residents to participate directly through influencing [65].

Even though security and privacy in a smart city can be perceived on various, but usually at least five layers [66], this study adds the layer of acceptance to the mix. The first layer encapsulates the ubiquitous, yet vulnerable physical sensors. The second layer refers to the collection of data from technological artefacts and sensors. The third layer relates to the networks that connect artefacts and sensors to servers, thus forming an integral part of the IoT ecosystem. The fourth layer is made up of computational sophistication and is responsible for processing data to support applications and services for the inhabitants. The fifth layer consists of providing services and smart applications that are tailored for residents. The sixth layer named acceptance refers to the cognitive state, or the degree to which smart city residents are willing or able to interact with the ecosystem. A summary of security threats is shown in Table 1.

Table 1. Summary of security threats.

Layer	Threat	Countermeasure
sensors	physical attacks on heterogeneous devices, hacking	robustness, monitoring, ubiquity
data	unauthorised access, eavesdropping, spoofing *, physical threats caused by environment and people	multi-factor verification and authentication, encryption, cryptography
network	malicious code insertion, signal jamming, wide range of hacking and cyber attacks, spoofing, sniffing °	data encryption, antivirus

Table 1. *Cont.*

Layer	Threat	Countermeasure
computing	denial of service, unauthorised access, insider threat, insecure software services	monitoring
services	DDoS, malicious code insertion, phishing, social engineering, spyware, cache overflow, backdoor, botnet	antiviruses, filters, user education, anti-DDoS measures
acceptance	influencing, lack of explainability, trust or meaningful control over systems	communication, training and education, user interfaces

* Spoofing is a broad term for the type of behaviour of a cybercriminal who impersonates a trusted entity or device.
° Sniffing occurs when an attacker intercepts and retrieves sensitive data passing through a network.

3.2. Privacy

This section discusses the most critical threats to data protection and privacy of residents in a smart city.

1. Identification: The threat of identification is related to the association of a person with private data. Authentication based on personal data minimisation limits the ability of sensors to collect data in the IoT, thus maintaining control over data disclosure [67].
2. Localisation: The threat of recording location or tracking a person's movement in space and time relates to the availability of spatio-temporal data in the IoT, where technological artefacts continuously record a user's identity, location, and activity [68].
3. Profiling: The threat of collecting and analysing data about the activities of individuals or groups in space and time, in order to identify their behaviours based on specific characteristics. The threat is exacerbated by identifying or combining it with other personal information [69].
4. Information fusion: The threat of creating accurate information as a result of combining independent data from different systems. The integration of different types of information about an individual that reveals new facts [70].
5. Exploitation: The threat of malicious use of personal information, leakage of personal data, creation of fake profiles, identity spoofing attacks, and misuse of facial recognition. Illegal collection of information about the existence and characteristics of specific persons and things. Unauthorised access to personal data that may be disclosed or leaked. Data that are subject to unprotected smart city infrastructure may provide information that facilitates the theft of personal data and its use for subversive activities.
6. Insecurity: The threat of not securing the sensors, technological artefacts, and software that are the starting point of any attack. If the hardware is not sufficiently tested, it poses a significant threat to the entire system. The lack of certification and standardisation of devices and software creates a vulnerability in the system, as an attack on one device can compromise the entire network [71]. Due to the large set of technological devices, a simple software bug can affect an entire system.
7. Extortion: A psychological threat that is compounded by the frequent interaction of smart city residents in the digital environment. Extortion can be perpetrated against individuals, but especially against children and adolescents. Such threats include child harassment, high-risk behaviour on social media, and communication with strangers [72].
8. Alteration of ownership: A threat based on a legal process in which a new person becomes the official owner of a technological artefact, sensor, system, or network that was previously used by another person. For example, an attacker could use hijacked smart metres to run ransomware on systems [73].
9. Influencing: Within the context of this study, this threat can be defined as a set of soft power instruments of influence that aim to obtain data or exploit system vulnerabilities to disrupt the processes of a smart city [74]. This can be achieved not

only by social engineering, but also by arousing negative sentiment, eroding residents' trust in governing institutions, or challenging core values of the concept [75].

10. Composite attacks: A combined threat consisting of multiple distributed attacks with a synergistic effect and a greater impact.

Examples of security and privacy threats in the context of different smart city domains and systems are shown in Table 2.

Table 2. Examples of security and privacy threats in the context of different smart city domains and systems.

System	Threat	Security Trends	Challenges
governance	combined attacks, extortion, insecurity, abuse	blockchain, cloudification, increase in computing capacity	Data immutability in blockchain depends on the distribution of nodes in a network. No entity shall own more than half.
residents	extortion, insecurity, abuse, information fusion, profiling, localisation, impersonation	biometrics, encryption, cryptography, data minimisation, anonymisation	Biometric databases represent a single point of failure. Biometrics are inherently publicly accessible.
economy	combined attacks, change of ownership, insecurity	blockchain, cloudification, artificial intelligence, machine learning	Cloudification increases latency, limits scalability, and creates a single point of failure.
housing	change of ownership, insecurity, profiling, localisation, identification	encryption, cryptography, security standards, attestation, authentication and validation	Cryptography is efficient but computationally intensive for personal devices.
healthcare	malware, phishing, insecurity, hacking, bioterrorism, ransomware	biometrics, robust artificial intelligence and machine learning models	Regulating adaptive AI algorithms. Periodically updating and configuring devices.
transportation	change of ownership, insecurity, profiling, localisation, identification	robust artificial intelligence and machine learning models, advanced mathematical models	The robustness of AI-based models depends on the amount of annotated and raw data used to train them.
environment	combined attacks, insecurity	sensorisation, artificial intelligence, machine learning	Periodically updating and configuring sensors. Standardisation and quality control.
finance	ransomware, phishing, spoofing, fraud, social engineering	multi-form authentication	Deploying digital currencies and modernising payment systems.

A summary of the general security and privacy requirements is as follows. Access to personal data should be restricted to owners or authorised individuals. Access should be based on identity verification and authorisation validation so that only authorised residents can access services through a structured system [76]. The performance of services should be contingent on the ability to monitor the conditions of their performance, which would allow for the detection of abnormalities and the identification of malpractice [77]. The availability of devices and services should be over-dimensioned so that intelligent systems or applications are redundant and able to be operative even during an attack or threat [78]. Hardware, communication networks, and software should be robust and have adequate resilience to physical damage [79]. Data exchange between sender and receiver shall be protected from malicious or unauthorised users. The potential risk of leakage and

disclosure of residents' personal information cannot be completely eliminated even in a secure system; hence it is advisable not to process all data through a single point, which could pose a weakness in the system [80]. In order to minimise the risk of leakage, rigorous testing should be part of the privacy design to verify that the system design does indeed meet the baseline requirements.

3.3. Cyber Threats

Cyber threats are addressed in a dedicated part because they represent a multifunctional tool that is capable of threatening all levels of security referred to in Section 3.1. Although cyber threats and vulnerabilities have a specific nature and form, it is difficult to quantify them within the scope of this work. The following is an approximation of some of the most common types of cyber threats that can be expected to seriously compromise the security of a smart city in Slovakia. The approximation also draws information from National Cyber Strategy Security for the years 2021 to 2025.

1. Short development cycle of new techniques and attack methods: The possibilities for attackers to use innovative tools are constantly improving. Therefore, the development of appropriate cybersecurity tools or the degree of their availability in specific markets may come too late or be of insufficient potency in some instances [81]. Attackers customarily react to emerging vulnerabilities in products and services in real time, while security measures can be subject to long development cycles. The development of emerging technologies such as applications of AI, quantum computing, and encryption further enables attackers to execute their attacks more efficiently. As vulnerability rates increase in direct proportion to the evolution of technology and the digitisation of society, accelerating development cycles exerts pressure on security requirements. This creates an asymmetry between dynamic development and the emphasis on security requirements, especially if the developer prioritises functionality and design over security. A similar problem arises in software technology upgrades, where improved functionality does not necessarily equate to better security, unless the very reason for the upgrade is security. Short development cycles also imply quicker loss of manufacturer support and infrequent updates for outdated products and services.

Slovakia is not developing competences and capabilities in the area of certification of products, processes, and services in the field of cybersecurity fast enough [82]. A consequence of this is the fact that service operators react vaguely and inflexibly to the obligation to develop adequate security measures, which is mainly due to the insufficient level of security awareness of operators and their suppliers in the field of cyber and information security [83]. Cybersecurity in the public administration has a complementary Act No. 95/2019 Coll. on Information Technology in Public Administration, but this regulation does not reflect the dynamically changing methods of attacks and is often not sufficiently implemented [82]. Furthermore, cyberspace is the domain of influence operations that, without an agile legislative response, are capable of compromising security through the proliferation of illegal content, disrupting public order, or undermining citizens' trust in smart city institutions.

2. Lack of expertise and low level of user awareness: Technological advances are not the only determinant of security; the human factor is equally important. Unless the individuals who handle technology and participate in the smart city ecosystem are competent or experienced enough to manage risks and apply security measures, the human factor will be a weak link in security [84]. Defining processes and implementing security measures require aware individuals as well as sufficient awareness in society to facilitate funding for security activities and ensure leadership support. For example, the detection of cyber incidents, i.e., attempted or successful attacks, is a challenging process, requiring a high level of expertise and technical capacity. Awareness of the pitfalls and risks in cyberspace affects not only the company but

also the users' attitude towards their own security. Individuals lacking knowledge and experience in cybersecurity can become ideal targets for attackers.

Professional education in the field of cybersecurity is not systematically addressed in the Slovak Republic, and there are very few university programmes in cybersecurity [85]. On top of that, cybersecurity research and development is decentralised and minimal, mainly carried out by private companies as part of their business activities and by academia [82]. The State does not have a coherent concept of support for cybersecurity R&D.

3. There is a slow implementation of legislative measures and standards. The topic of security is not commonly considered a priority, but mostly just an obligation that must be fulfilled by law; implementing regulations or non-legislative standards defines the status quo of measures across all levels of security. Moreover, legislative cycles are usually much longer than the cycle of innovation and application of new methods and technologies in the cybercrime field [86].

The implementation of security measures is a structured operation, which is determined by law, implementing regulations or a non-legislative standard. Slovakia relies heavily on the citizen itself as the end user of any security services. Although cybercrime is well established in legislation, the practical enforcement of the law in this area faces legislative obstacles [82]. The problem is exacerbated because of a wide variation in cybersecurity and the implementation of security measures by operators of essential services across different sectors [87].

4. Discussion

In order to discuss the challenges and open issues in the researched area, the discussion of this work deals with the search for a comprehensive privacy protection method that takes into account the most important specificities of the Slovak smart city security landscape.

4.1. Data-Centric Approach

Due to the large volume of managed data, the complexity of interconnected networks, technologies, and users in a smart city and their privacy presents a target for a wide range of attacks and malicious activities. Creating reliable methods to secure and protect privacy in smart cities is a complex task. Threats to this smart platform occur across the entire spectrum of processes, from data collection, processing and transmission to technical infrastructure including the residents. The most important prerequisite of a secure smart city concept should be incorporating privacy requirements into the design of systems and their interactions. To minimise the leakage of sensitive information, different aspects of cyber-security and privacy protection must be intertwined. Residents' requirements need to be understood and translated into sound design of an architecture that describes system components, their responsibilities, and the relationships in between them.

Residents should have the right to transfer their data from one service provider to another or to delete their data entirely. Each individual has their own privacy needs and requirements, so services should have privacy configurability and notify users if this is not possible. In an ideal smart city, residents will be able to opt out of using the services completely and have the option to completely delete all data collected about them. Data protection also applies to systems that disclose information beyond privacy at first glance. This is mainly due to the possibility of combining seemingly non-private and non-personal data from multiple sources, which can lead to the disclosure of sensitive information or the creation of user profiles.

Functionality of smart city processes should be continuously reviewed, specifically the alignment of processes with the main objective of the model, which is to improve services for residents. Responsible use and handling of citizens' data by smart city authorities and service providers as well as the compliance with privacy principles by the residents themselves who are held accountable strikes a balance within the system [88]. Lastly, an audit brings a measure of transparency to the model through clarification of processes. The

audit should not only be able to clarify eventualities in which privacy has been breached and identify leaked data, but also specify how often privacy attacks occur, whether they are effective, and to what extent the security system is able to resist or mitigate attacks. Understanding data management is important because users need to know where data are stored, with whom it is shared, what it is used for, and how it is protected. In a smart city, data are collected in the hands of authorities and service providers making it difficult for individuals to verify all aspects related to its management due to the systemic complexity. Transparency will increase the level of trust among residents and thus increase the level of participation of residents in the use of smart services. Privacy should be understandable to users from a methodological and systemic point of view [89].

4.2. Resident-Centric Approach

The conceptual model should be based on a user-oriented approach, which relates to the management of the trust and acceptance mentioned in the previous paragraphs. In practice, this means that at each level of smart services, residents should receive personalised or be able to personalise their privacy and data sharing settings through adequate user interfaces. Services provided for residents should reflect the security preferences and interests of smart city residents. Vice versa, residents should maintain meaningful control over systems that provide them with welfare surplus. Users should be able to manage and control their data and determine the degree of their granularity. For example, define access level options for authorised individuals, authorised applications, and data accuracy definitions. An example of customising privacy settings for mobile users could be to provide different accesses to device location information, for example, family and close friends have access to exact location, smart city authorities and third-party services have access to location with a large deviation, and other entities do not have access at all.

This work argues for a user-oriented approach that considers a cognitive layer or acceptance of residents to actively participate as an important aspect outside the conventional security and privacy protection scope. The smart city as a set of interconnected systems is not so different from the states. In recent years, the number and range of influencing activities has been growing. The application of these methods has been made possible mainly by digitalisation and technological advances, which have not only brought new possibilities of activities and attack vectors into the information space, but also reduced the technological and financial requirements for their implementation. Influence attacks on citizens can have the same impact on the security interests of cities and countries as conventional or cyber-attacks.

Instead of using sophisticated cyber-attacks, it may be cheaper and more effective to use a wide range of influence techniques and tools, such as spreading disinformation, radicalising citizens, exerting pressure on city government officials or institutions, and creating public unrest in the targeted smart city. Through these techniques, malicious actors are able to undermine and subvert the functioning of systems from within. Even the Slovak Republic is not immune to such influence operations. On the contrary, NATO's Annual Tracking Research 2022 suggests that Slovak citizens are highly susceptible to such threats. In general, these influence operations are carried out in a coordinated manner below the threshold of a normal response in a democratic city governed by the rule of law. Due to their complex nature and difficult detection, influence operations are difficult for the general public to detect and understand, increasing the likelihood that they will eventually succumb to them.

One of the main tools of the struggle that the smart city has in its hands is communication. Through it, trust is fostered, as well as the value base and the resilience of citizens to subversive influences that seek to undermine it. Today, through technology, city and municipal leaders are able to reach specific target groups quickly. Well-executed communication brings coherence to the implementation of norms or standards, looks beyond the everyday, seeks to direct the target audience towards a long-term change in mindset, and

presents the benefits of a smart city ecosystem, long-term vision, and policy priorities to its residents in a compelling manner.

4.3. Policy-Centric Approach

In terms of standards, laws, and policies, data management in a smart city ecosystem requires a non-technical form of guidance throughout the entire lifecycle, from generation, use, dissemination, and classification to storage. A well-defined and enforceable law minimises opportunities for data misuse and ensures that stakeholders accept and respect ethical standards. Non-technical mechanisms function as a complement to technical mechanisms and should therefore be carefully designed with the comprehensive security and privacy mechanism of a smart city in mind. Non-technical standards for smart city implementation on a global scale have not yet been widely accepted and used due to lack of elaboration and absence of international consensus on terminology [90]. Standards, laws, and policies are only formulated and implemented locally.

While reflecting on the current state of policies, public administration, information system architecture, implemented development projects, and municipal activities, and extending them with new principles resulting from current trends in the Slovak Republic, the smart city pertinent policies that relate to education, digitalisation, and security in public administration seem to be rather disjointed and compartmentalised for individual public administration programmes. New modernisation pressures are currently compelling public institutions to streamline the performance of all their legislative actions, their accountability, and the public's participation in the process. Moreover, being part of the so-called European administrative area changes the meaning, content, and standards of good governance law, which requires a high level of knowledge and commitment of public authorities who are, according to the statistics of the Ministry of Education, not supported by a sufficient number of experts in the field of cyber and information security. Future policies must focus on improving the conditions for the adoption of digitisation, innovativeness, and competitiveness by reducing administrative burdens, making legislative and policy changes, defining standards, and reforming the education curriculum and the labour market.

Slovak legislature enables potential development of smart cities to a reasonable extent. In spite of this, a challenge has also been identified, namely, the general fragmentation of the Slovak legislation. In addition, there are too many unlinked strategic and conceptual documents that are not sufficiently updated to meet the needs of the immediate realities of the situation or do not provide sufficiently targeted solutions. The policies are not comprehensible to the citizens, which undermines their credibility. Last but not least, Slovakia is a weak absorber of EU funds, despite the fact that sustainable and integrated development of urban and rural areas through local initiatives is one of its priorities. According to the Ministry of Finance, there is still almost unspent EUR 7 billion (approx. 50%) from the previous programming period. In order to achieve the prerequisites for smart cities before the start of the new programming period 2021–2027, the work stresses the need to simplify, streamline, and make transparent the process of spending smart city relevant EU funding.

5. Conclusions

This work has identified smart city governance, residents, economy, housing, healthcare, transportation, infrastructure, environment, and finance as the most important smart city domains that can become subject to attacks. The security requirements for the abovementioned systems should address the assurance of the following parameters: active participation of residents, meaningful human control, technology and user connectivity, scalability, data security, system heterogeneity, hardware constraints, autonomy, and physical vulnerability. Security and privacy in a smart city can be perceived at the physical layer, data layer, network layer, computing layer, the services layer, and user acceptance layer. The most critical threats to security and privacy include user identification, user

localisation, user profiling, user influencing, user extortion, data association, data misuse, data insecurity, change of device ownership, and combining attacks. Smart cities are particularly vulnerable to cyber-attacks due to the short development cycle of new techniques and methods of attack, the lack of expertise and low level of user awareness, and slow pace of implementation of legislative measures, norms, and standards.

Considering possibilities, assumptions, problems, and factors of its feasibility in the Slovak Republic, this work identified and discussed data, residents, and policies as key aspects to sustainable smart city development. Acceptance of the smart city concept by residents and the role of meaningful human control over smart city systems are ensuring that residential participation in the smart city ecosystem were added to the results derived from literature research. Beyond sophisticated cyber-attacks or social engineering, this work added influence activities to the list of potential threats, as based on the research and fact that Slovak citizens are highly susceptible to influencing and the fact that influencing efficacy in destabilising smart cities may be higher than conventional methods. Simple communication was identified as one of the main tools that the smart city administrations have at their disposal to counter threats to smart city security. Slovak legislature enables implementation of generic conceptual models for smart cities. Nonetheless, fragmentation of relevant legislation was identified as a challenge. Furthermore, diverging strategic documents must be updated and interwoven to better specify tasks, manner, and time frame for their implementation and responsibility of actors. The policies seem to be incomprehensible to the citizens, which undermines their credibility. Lack of expertise and user awareness, professional education as well as a short development cycle of new attack methods are all risk factors linked with the slow implementation of legislative measures.

After describing smart city systems and identifying threats in the previous parts of this work, the process-based and data-driven approaches that are important for an acceptable privacy mechanism are as follows. A smart city concept needs to place adequate emphasis on the security and privacy of its inhabitants, especially to ensure their trust and active participation in the digital ecosystem. Ideally, the concept of security and privacy in a smart city should be cross-cutting, where security requirements should be an inherent part of its design. In practice, this means that a secure conceptual model of a smart city should constitute the starting point for the functionality of all systems and, in addition, should be tailored to the specific needs of the residents. For the long-term sustainability of the conceptual model, it is essential to conduct responsible auditing as well as regular testing and verification of its functionality. Furthermore, auditing leads to increased transparency. Protecting residents means placing particular emphasis on data protection by integrating security requirements into software and engineering processes. Technical mechanisms must be supported by non-technical ones in the form of norms, standards, legislation, and agile policies that match the pace of innovation and development. Plurality of service providers and market competition is a beneficial factor for sustainability. Users should be able to manage or permanently erase data collected by authorities and service providers at any time.

There are three limitations to this study. Firstly, literature about smart cities in Slovakia and case studies dealing with Slovak context are limited, thus conclusions are subjected to bias. Secondly, the mixed research method combined systematic review of a wide scope of smart city aspects with considerations for their possibilities, assumptions, problems, and factors of feasibility in Slovakia, which made it difficult to analyse all security layers and requirements in high detail, which results in generalised discussion and conclusions. Thirdly, the work utilises systematic review mainly as a reference point for investigating the many aspects of smart cities in Slovakia. Given that the information is relevant in relation to the specific, it would be beyond the scope of the work to excessively compare, cross-reference, or critically evaluate the default information generated in the literature review.

The subject of future research may be to investigate a specific area of smart city security in Slovakia from a set perspective, for example, the effect of influence operations on the

stability of the smart city concept; another option might be to approach the topic of smart city cybersecurity in Slovakia from a more multi-disciplinary perspective.

Author Contributions: Conceptualisation, M.K., T.G., S.S. and J.R.; methodology, M.K. and J.R.; validation, M.K. and S.S.; formal analysis, T.G.; investigation, M.K.; resources, S.S.; writing—original draft preparation, M.K., T.G. and J.R.; writing—review and editing, S.S.; visualisation, T.G.; supervision, J.R.; project administration, J.R.; funding acquisition, J.R. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Scientific Grant Agency of the Ministry of Education, Science, Research and Sport of the Slovak Republic—VEGA No. 1/0459/21, "Proposal of Adaptation Measures for the Reduction of Risks Arising from Climate Change from the Point of View of the Occurrence of Crisis Phenomena and Weather Extremes" and the Educational Grant Agency of the Ministry of Education, Science, Research and Sport of the Slovak Republic—KEGA No. 043ŽU-4/2022, "Implementation of Knowledge from Social, Behavioural and Humanities Disciplines in the Preparation of Students in the Field of Safety and Security Sciences".

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable, as all the relevant information can be found in the article.

Acknowledgments: The views expressed are solely those of the authors and not necessarily those of the institutions with which they are affiliated or of their funding sources. The authors are solely responsible for any errors or omissions.

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

References

1. Picon, A. Opinions, Smart Cities, Privacy and the Pulverisation/Reconstruction of Individuals. *Eur. Data Prot. Law Rev.* **2019**, *5*, 154–155. [CrossRef]
2. Komninos, N. What Makes Cities Intelligent? In *Smart Cities: Governing, Modelling and Analysing the Transition*; Deakin, M., Ed.; Taylor and Francis: Abingdon, UK, 2013; p. 77.
3. Alter, S. Making Sense of Smartness in the Context of Smart Devices and Smart Systems. *Inf. Syst. Front.* **2020**, *22*, 381–393. [CrossRef]
4. Seta, F.; Sen, J.; Biswas, A.; Khare, A. *From Poverty, Inequality to Smart City Proceedings of the National Conference on Sustainable Built Environment 2015*, 1st ed.; Seta, F., Sen, J., Biswas, A., Khare, A., Eds.; Springer: Singapore, 2017.
5. Yeh, H. The effects of successful ICT-based smart city services: From citizens' perspectives. *Gov. Inf. Q.* **2017**, *34*, 556–565. [CrossRef]
6. McLaren, D.; Agyeman, J. *Sharing Cities: A Case for Truly Smart and Sustainable Cities/Duncan McLaren and Julian Agyeman*; MIT Press: Cambridge, MA, USA, 2015.
7. Vinod Kumar, T.M. (Ed.) *Smart Living for Smart Cities Case Studies*, 1st ed.; Springer: Singapore, 2020.
8. AI-Turjman, F.; Imran, M. (Eds.) *IoT Technologies in Smart Cities from Sensors to Big Data, Security and Trust*; IET: Stevenage, UK, 2020.
9. Ejaz, W.; Anpalagan, A. (Eds.) *Internet of Things for Smart Cities Technologies, Big Data and Security*, 1st ed.; Springer International Publishing: Cham, Switzerland, 2019.
10. Orlowski, C. *Management of IOT Open Data Projects in Smart Cities*; Elsevier Science & Technology: San Diego, CA, USA, 2020.
11. Ju, J.; Liu, L.; Feng, Y. Citizen-centered big data analysis-driven governance intelligence framework for smart cities. *Telecommun. Policy* **2018**, *42*, 881–896. [CrossRef]
12. 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]
13. Rizi MH, P.; Seno SA, H. A systematic review of technologies and solutions to improve security and privacy protection of citizens in the smart city. *Internet Things* **2022**, *20*, 100584. [CrossRef]
14. Orłowski, C. *Management of IoT Open Data Projects in Smart Cities Cezary Orlowski*; Academic Press: London, UK, 2021.
15. Popkova, E.G.; Polukhin, A.A.; Ragulina, J.V. *Towards an Increased Security: Green Innovations, Intellectual Property Protection and Information Security*; Springer International Publishing: Cham, Switzerland, 2022; Volume 372.
16. Srebalová, M.; Peráček, T. Effective Public Administration as a Tool for Building Smart Cities: The Experience of the Slovak Republic. *Laws* **2022**, *11*, 67. [CrossRef]

17. Cagáňová, D. *Smart Technology Trends in Industrial and Business Management Edited by Dagmar Cagáňová, Michal Balog*, 1st ed.; Knapčíková, L., Soviar, J., Mezarcıöz, S., Cagáňová, D., Eds.; Springer International Publishing: Cham, Switzerland, 2019.
18. Yigitcanlar, T.; Yigitcanlar, T. *Reviews and Perspectives on Smart and Sustainable Metropolitan and Regional Cities*; MDPI—Multidisciplinary Digital Publishing Institute: Basel, Switzerland, 2021.
19. Lacinák, M.; Ristvej, J. Smart City, Safety and Security. *Procedia Eng.* **2017**, *192*, 522–527. [CrossRef]
20. Fabrègue, B.F.G.; Bogoni, A. Privacy and Security Concerns in the Smart City. *Smart Cities* **2023**, *6*, 586–613. [CrossRef]
21. Sicari, S.; Rizzardi, A.; Grieco, L.A.; Coen-Porisini, A. Security, privacy and trust in Internet of Things: The road ahead. *Comput. Netw.* **2015**, *1999*, 76146–76164. [CrossRef]
22. Gharaibeh, A.; Salahuddin, M.A.; Hussini, S.J.; Khreishah, A.; Khalil, I.; Guizani, M.; Al-Fuqaha, A. Smart Cities: A Survey on Data Management, Security, and Enabling Technologies. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 2456–2501. [CrossRef]
23. 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]
24. Eckhoff, D.; Wagner, I. Privacy in the Smart City-Applications, Technologies, Challenges, and Solutions. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 489–516. [CrossRef]
25. Bolivar, M.P.R.; Meijer, A.J. Smart Governance: Using a Literature Review and Empirical Analysis to Build a Research Model. *Soc. Sci. Comput. Rev.* **2016**, *34*, 673–692. [CrossRef]
26. Vitálišová, K.; Vaňová, A.; Borseková, K.; Nagyová, Ľ.; Cagáňová, D. Tools of Smart Governance in Cities of the Slovak Republic. In *Science and Technologies for Smart Cities*; Springer International Publishing: Cham, Switzerland, 2019; pp. 369–387.
27. Shaw, S.-L.; Sui, D. *Human Dynamics Research in Smart and Connected Communities*; Springer International Publishing AG: Cham, Switzerland, 2018.
28. Vinod Kumar, T.M. (Ed.) *Smart Economy in Smart Cities: International Collaborative Research: Ottawa, St. Louis, Stuttgart, Bologna, Cape Town, Nairobi, Dakar, Lagos, New Delhi, Varanasi, Vijayawada, Kozhikode, Hong Kong*, 1st ed.; Springer: Singapore, 2017.
29. Mboup, G.; Oyelaran-Oyeyinka, B. (Eds.) *Smart Economy in Smart African Cities Sustainable, Inclusive, Resilient and Prosperous*, 1st ed.; Springer: Singapore, 2019.
30. Li, X.; Lu, R.; Liang, X.; Shen, X.; Chen, J.; Lin, X. Smart community: An internet of things application. *IEEE Commun. Mag.* **2011**, *49*, 68–75. [CrossRef]
31. Sheina, S.; Fedorovskaya, A.; Yudina, K. Smart City: Comfortable Living Environment. *IOP Conf. Ser. Mater. Sci. Eng.* **2018**, *463*, 32095. [CrossRef]
32. Cui, L.; Xie, G.; Qu, Y.; Gao, L.; Yang, Y. Security and Privacy in Smart Cities: Challenges and Opportunities. *IEEE Access* **2018**, *6*, 46134–46145. [CrossRef]
33. Zhao, W.; Luo, X.; Qiu, T. (Eds.) *Recent Developments in Smart Healthcare*; MDPI—Multidisciplinary Digital Publishing Institute: Basel, Switzerland, 2018.
34. Ševcová, K. Digitalization of the Health Care System in the Slovak Republic. *Rev. Int. Jurídica Empresarial* **2020**, *3*, 45–60. [CrossRef]
35. Kostakos, V.; Ojala, T.; Juntunen, T. Traffic in the Smart City: Exploring City—Wide Sensing for Traffic Control Center Augmentation. *IEEE Internet Comput.* **2013**, *17*, 22–29. [CrossRef]
36. Golej, J.; Pánik, M.; Špirková, D.; Adamuscin, A. Smart Mobility in Urban Development. In *Advances in Human Factors in Architecture, Sustainable Urban Planning and Infrastructure*; Springer International Publishing: Cham, Switzerland, 2020; pp. 192–198.
37. Ristvej, J.; Lacinák, M.; Ondrejka, R. On Smart City and Safe City Concepts. Mobile Networks and Applications. *Mob. Netw. Appl.* **2020**, *25*, 2020. [CrossRef]
38. Rehak, D.; Hromada, M.; Lovecek, T. Personnel Threats in an Electric Power Critical Infrastructure Sector and Their Impacts on Dependent Sectors. *Saf. Sci.* **2020**, *127*, 104698. [CrossRef]
39. Janíček, F.; Perný, M.; Šály, V.; Váry, M.; Breza, J.; Chochol, P. The role of smart grid in integrating the renewable energies in Slovakia. *Energy Environ.* **2018**, *29*, 300–312. [CrossRef]
40. Shen, Z.; Huang, L.; Peng, K.H.; Pai, J. (Eds.) *Green City Planning and Practices in Asian Cities Sustainable Development and Smart Growth in Urban Environments*, 1st ed.; Springer International Publishing: Cham, Switzerland, 2018.
41. Brezula, J. Aspects of cyber security in Slovakia and in the world. *Krízový Manažment* **2017**, *16*, 83–88. [CrossRef]
42. Ahram, T.; Taiar, R. Human Interaction, Emerging Technologies and Future Applications III. In Proceedings of the 3rd International Conference on Human Interaction and Emerging Technologies: Future Applications (IHIET 2020), Paris, France, 27–29 August 2020; Ahram, T., Taiar, R., Langlois, K., Choplin, A., Eds.; Springer International Publishing: Cham, Switzerland, 2021.
43. Yarali, A. (Ed.) *Intelligent Connectivity: AI, IoT, and 5G*; Wiley: Hoboken, NJ, USA, 2022.
44. Dogra, R.; Rani, S.; Sharma, B.; Verma, S. Essence of Scalability in Wireless Sensor Network for Smart City Applications. *IOP Conf. Ser. Mater. Sci. Eng.* **2021**, *1022*, 12094. [CrossRef]
45. Haj Qasem, M.; AlMobaideen, W. Heterogeneity in IoT-based Smart Cities Designs. *Int. J. Interact. Mob. Technol.* **2019**, *13*, 210–225. [CrossRef]
46. Šulyová, D.; Kubina, M. Integrated management of limited water resources in Smart Cities. *IOP Conf. Ser. Earth Environ. Sci.* **2022**, *1077*, 012003. [CrossRef]
47. Kulhari, S. (Ed.) *Building-Blocks of a Data Protection Revolution: The Uneasy Case for Blockchain Technology to Secure Privacy and Identity*, 1st ed.; Nomos Verlagsgesellschaft mbH & Co. KG: Baden-Baden, Germany, 2018.

48. Kampova, K.; Lovecek, T.; Rehak, D. Quantitative approach to physical protection systems assessment of critical infrastructure elements: Use case in the Slovak Republic. *Int. J. Crit. Infrastruct. Prot.* **2020**, *30*, 100376. [CrossRef]
49. Sheng, Z.; Yang, S.; Yu, Y.; Vasilakos, A.V.; McCann, J.A.; Leung, K.K. A survey on the ietf protocol suite for the internet of things: Standards, challenges, and opportunities. *IEEE Wirel. Commun.* **2013**, *20*, 91–98. [CrossRef]
50. Xu, K.; Wang, X.; Wei, W.; Song, H.; Mao, B. Toward software defined smart home. *IEEE Commun. Mag.* **2016**, *54*, 116–122. [CrossRef]
51. 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; pp. 1392–1393.
52. Kasaraneni, P.P.; Yellapragada, V.P.K.; Moganti, G.L.K.; Flah, A. Analytical Enumeration of Redundant Data Anomalies in Energy Consumption Readings of Smart Buildings with a Case Study of Darmstadt Smart City in Germany. *Sustainability* **2022**, *14*, 10842. [CrossRef]
53. Visvizi, A.; Lytras, M.D. (Eds.) *Sustainable Smart Cities and Smart Villages Research*; MDPI—Multidisciplinary Digital Publishing Institute: Basel, Switzerland, 2018.
54. Yigitcanlar, T.; Han, H.; Kamruzzaman, M. *Approaches, Advances and Applications in Sustainable Development of Smart Cities*; MDPI—Multidisciplinary Digital Publishing Institute: Basel, Switzerland, 2020.
55. Kitchenham, B.A. Procedures for Performing Systematic Reviews. Joint Technical Report, Computer Science Department, Keele University (TR/SE0401) and National ICT Australia Ltd. (0400011T.1). 2004. Available online: http://www.inf.ufsc.br/~aldo.vw/kitchenham.pdf (accessed on 27 February 2020).
56. Moher, D.; Liberati, A.; Tetzlaff, J.; Altman, D.G. Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. *Ann. Intern. Med.* **2009**, *151*, 264–269. [CrossRef] [PubMed]
57. O'Brien, A.M.; Mc Guckin, C. *The Systematic Literature Review Method: Trials and Tribulations of Electronic Database Searching at Doctoral Level*; O'Brien, A.M., Ed.; SAGE Publications: London, UK, 2016.
58. Boland, A.; Cherry, G.; Dickson, R. (Eds.) *Doing a Systematic Review: A Student's Guide*, 2nd ed.; SAGE: Los Angeles, CA, USA, 2017.
59. Hesse-Biber, S.N.; Johnson, B. (Eds.) *The Oxford Handbook of Multimethod and Mixed Methods Research Inquiry*; Oxford University Press: New York, NY, USA, 2016.
60. Heyvaert, M.; Hannes, K.; Onghena, P. (Eds.) *Using Mixed Methods Research Synthesis for Literature Reviews*; SAGE: Los Angeles, CA, USA, 2017.
61. Singh, S.; Sharma, P.K.; Moon, S.Y.; Moon, D.; Park, J.H. A comprehensive study on APT attacks and countermeasures for future networks and communications: Challenges and solutions. *J. Supercomput.* **2019**, *75*, 4543–4574. [CrossRef]
62. Alandjani, G. Features and Potential Security Challenges for IoT Enabled Devices in Smart City Environment. *Int. J. Adv. Comput. Sci. Appl.* **2018**, *9*, 8. [CrossRef]
63. Belous, A.; Saladukha, V. (Eds.) *Viruses, Hardware and Software Trojans Attacks and Countermeasures*, 1st ed.; Springer International Publishing: Cham, Switzerland, 2020.
64. da Costa, K.A.P.; Papa, J.P.; Lisboa, C.O. Internet of Things: A survey on machine learning-based intrusion detection approaches. *Comput. Netw.* **1999**, *151*, 147–157. [CrossRef]
65. Siman, B. *Hybrid Warfare Is Not Synonymous with Cyber: The Threat of Influence Operations*; EGMONT Royal Institute for International Relations: Brussels, Belgium, 2022.
66. Ying, B. Privacy preserving broadcast message authentication protocol for VANETs. *J. Netw. Comput. Appl.* **2013**, *36*, 1352–1364. [CrossRef]
67. Al-Dhubhani, R.; Mehmood, R.; Katib, I.; Algarni, A. Location Privacy in Smart Cities Era. In *Smart Societies, Infrastructure, Technologies and Applications*; Springer International Publishing: Cham, Switzerland, 2018; pp. 123–138.
68. Antonopoulos, K.; Petropoulos, C.; Antonopoulos, C.P.; Voros, N. Security Data Management Process and Its Impact on Smart Cities' Wireless Sensor Networks. In Proceedings of the 2017 South Eastern European Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM) 2017, Preveza, Greece, 23–25 September 2017; pp. 1–8.
69. Beltran, V.; Martinez, J.A.; Skarmeta, A. User-Centric Access Control for Efficient Security in Smart Cities. In Proceedings of the 2017 Global Internet of Things Summit (GIoTS), Geneva, Switzerland, 6–9 June 2017; IEEE: Piscataway, NJ, USA; pp. 1–6.
70. Ali, H.; Elzeki, O.M.; Elmougy, S. Smart Attacks Learning Machine Advisor System for Protecting Smart Cities from Smart Threats. *Appl. Sci.* **2022**, *12*, 6473. [CrossRef]
71. Huang, Q.; Wang, L.; Yang, Y. Secure and Privacy-Preserving Data Sharing and Collaboration in Mobile Healthcare Social Networks of Smart Cities. *Secur. Commun. Netw.* **2017**, *2017*, 6426495. [CrossRef]
72. Gheisari, M.; Wang, G.; Khan, W.Z.; Fernández-Campusano, C. A context-aware privacy-preserving method for IoT-based smart city using Software Defined Networking. *Comput. Secur.* **2019**, *87*, 101470. [CrossRef]
73. Alromaihi, S.; Elmedany, W.; Balakrishna, C. Cyber Security Challenges of Deploying IoT in Smart Cities for Healthcare Applications. In Proceedings of the 2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Barcelona, Spain, 6–8 August 2018; pp. 140–145.
74. Gressel, G. *Protecting Europe against Hybrid Threats*; European Council on Foreign Relations: Berlin, Germany, 2022.

75. Sweijs, T. *Framework for Cross-Domain Strategies Against Hybrid Threats*; Hague Centre for Strategic Studies: The Haag, The Netherlands, 2022.
76. Sarri, A.; Kyranoudi, P. *Good Practices in Innovation on Cybersecurity under the NCSS: Good Practices in Innovation on Cybersecurity under the National Cyber Security Strategies*; ENISA_2: Heraklion, Greece, 2019.
77. Nicholson, D. Advances in Human Factors in Cybersecurity. In *Proceedings of the AHFE 2017 International Conference on Human Factors in Cybersecurity, Los Angeles, CA, USA, 17−21 July 2017*, 1st ed.; Nicholson, D., Ed.; Springer International Publishing: Cham, Switzerland, 2018.
78. Poehlmann, N.; Caramancion, K.M.; Tatar, I.; Merz, T. The Organizational Cybersecurity Success Factors: An Exhaustive Literature Review. In *Advances in Security, Networks, and Internet of Things*; Springer International Publishing: Cham, Switzerland, 2021; pp. 377–395.
79. Kalyani, G.; Chaudhari, S. An efficient approach for enhancing security in Internet of Things using the optimum authentication key. *Int. J. Comput. Appl.* **2020**, *42*, 306–314. [CrossRef]
80. Chatterjee, S.; Kar, A.K.; Gupta, M.P. Alignment of IT Authority and Citizens of Proposed Smart Cities in India: System Security and Privacy Perspective. *Glob. J. Flex. Syst. Manag.* **2018**, *19*, 95–107. [CrossRef]
81. 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. *Future Gener. Comput. Syst.* **2020**, 112724–112737. [CrossRef]
82. National Security Authority. National Cyber Strategy Security for the Years 2021 to 2025. Available online: https://www.nbu.gov.sk/wp-content/uploads/cyber-security/National_cybersecurity_strategy_2021.pdf (accessed on 12 December 2022).
83. Kamil, H.; Burita, L.; Kozak, P. Overview of Cyber Threats in Central European Countries. In Proceedings of the 2021 Communication and Information Technologies (KIT), Vysoke Tatry, Slovakia, 13–15 October 2021; pp. 1–6.
84. Sharma, A.; Singh, Y. On Security of Opportunistic Routing Protocol in Wireless Sensor Networks. In *Proceedings of ICRIC 2019*; Springer International Publishing: Cham, Switzerland, 2019; pp. 407–419.
85. Nagy, M. Cyber Security Strategies of the Visegrád Group States and Romania. *Acta Univ. Sapientiae Eur. Reg. Stud.* **2021**, *19*, 72–87. [CrossRef]
86. Fadlullah, Z.M.; Khan Pathan, A.-S. (Eds.) *Combating Security Challenges in the Age of Big Data Powered by State-of-the-Art Artificial Intelligence Techniques*, 1st ed.; Springer International Publishing: Cham, Switzerland, 2020.
87. Viano, E.C. (Ed.) *Cybercrime, Organized Crime, and Societal Responses International Approaches*, 1st ed.; Springer International Publishing: Cham, Switzerland, 2017.
88. Vitunskaite, M.; He, Y.; Brandstetter, T.; Janicke, H. Smart cities and cyber security: Are we there yet? A comparative study on the role of standards, third party risk management and security ownership. *Comput. Secur.* **2019**, *83*, 313–331. [CrossRef]
89. Sanduleac, M. Energy ecosystem in smart cities—Privacy and security solutions for citizen's engagement in a multi-stream environment. In Proceedings of the 2016 IEEE International Smart Cities Conference (ISC2), Trento, Italy, 12–15 September 2016; pp. 1–4.
90. Van den Broek, T.; van Veenstra, A.F. Governance of big data collaborations: How to balance regulatory compliance and disruptive innovation. *Technol. Forecast. Soc. Change* **2018**, *129*, 330–338. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.