



UDK: 351.777.81:[711.45:004.7

COBISS.SR-ID 148901385

DOI: 10.5281/zenodo.12614831

Review paper

WEAK POINTS OF SMART CITIES

Milica Varšandan⁵¹; Čaba Varšandan⁵²; Draško Vidović⁵³; Duško Bogdanić⁵⁴

Abstract

Smart cities represent an innovative approach to urban planning and general infrastructure management. Advanced technologies are used to improve the quality of life of all citizens. Regardless of the promising aspects, implementations of smart cities, and even the very meaning of the phrase “smart city”, face a number of challenges that require careful considerations. This paper gives some ideas about the weaknesses of smart cities. We consider the subject of privacy, risks arising from security issues, digital divide (i.e., the types of permanent distributions of people it can cause), dependences caused by the technology, additional costs and necessary financing, the necessary regulations that do not exist, and some standards that are in the process of implementation but are not mature enough. By analyzing all the known aspects, we will emphasize the need for an approach that includes authorities, industries, academic communities, and, of course, all other citizens. We will try to disclose some suggestions that can serve as an initial strategy or initial guidelines for a better tomorrow. Without such efforts, smart cities would not be able to become technologically advanced and at the same time to be sustainable and resistant to the challenges of the future.

Keywords: *smart cities, challenges, weaknesses, security approaches.*

Introduction

With the development of technology, digitalization, the growth of the Internet of Things (IoT) and big data, smart cities have started to develop. All this development has happened in the last few decades. Big cities began to use smart solutions as the technologies became more available and affordable.

⁵¹ Milica Varšandan, 1989, Faculty of Mathematics and Computer Science, Alfa BK University, milicamarjanovic@alfa.edu.rs <https://orcid.org/0009-0002-6500-2464>

⁵² Čaba Varšandan, 1987, HTEC Group doo, Serbia, varsandancaba@gmail.com <https://orcid.org/0009-0009-4321-9276>

⁵³ Draško Vidović, Monash University, Australia, drasko.vidovic@monash.edu <https://orcid.org/0000-0003-4269-3995>

⁵⁴ Duško Bogdanić, 1981, PhD, Alfa BK University, duško.bogdanic@alfa.edu.rs <https://orcid.org/0000-0002-6511-7475>



The development of smart cities began in Los Angeles in the late sixties and early seventies of the last century [1]. The data were collected on traffic density, pollution levels, and social tensions throughout the city, and in order to make people's lives easier, projects were initiated to improve public transport and reduce air pollution. This project is called Los Angeles Cluster Analysis [2], [5]. That was probably the first time the idea of a smart city was developed, although the term “Smart City” had not yet been defined.

In 1994, Amsterdam was the first to create a virtual city. Inspired by those events in Los Angeles and Amsterdam, the idea of creating smart cities came about. The idea of smart cities then continued to develop, technologies developed at a high speed and ideas just kept coming.

“There are five main components that are essentially required to be in a smart city: modern information and communication technologies, buildings, utilities and infrastructure, transportation and traffic management, and the city itself. A technically smart city refers to the cooperation between management institutes and public and private foundations for the implementation and application of long-term computerized platforms that are imposed using modern technologies, electronic facilities, networks and intelligent decision-making methodology.” [3].

Important aspects to consider

When considering smart cities, although they offer many advantages, there are also certain weaknesses and challenges to consider:

- 1. Data privacy:** Smart cities generate large amounts of data through sensors, smart devices, and network infrastructure. Protection of data privacy becomes crucial, and insufficient protection can lead to misuse or unauthorized access to sensitive information of citizens.
- 2. Security:** Given the interconnectedness of many systems in smart cities, there is an increased risk of cyber attacks. In particular, such attacks, e.g. hacking traffic systems, energy infrastructure or communication networks, can have serious consequences.
- 3. Digital divide:** Smart cities can widen the gap between those who have access to technology and digital resources and those who do not. This can lead to an increase in social inequalities if digital innovations are not implemented in a way that is accessible to all citizens.
- 4. Dependence on technology:** Dependence on technology in smart cities can lead to problems if there is a malfunction or interruption in the network. For example, breakdowns in public transport systems or energy networks can have serious consequences for citizens.



5. Costs and Financing: Implementing smart technologies can be expensive, and cities can face the challenge of securing sufficient funds to finance these projects. Lack of financial resources can limit cities' ability to realize their smart visions.

6. Regulation and standardization: The lack of clear regulation and standardization can hinder interoperability between different systems and technologies in smart cities. This can create problems in managing and integrating different aspects of smart infrastructure.

7. Disaster resilience: Smart cities should be resilient to natural disasters and crisis situations. Lack of adequate emergency planning can lead to serious consequences in the event of floods, hurricanes, earthquakes, or other unforeseen events.

Data privacy

In everyday life, people living in a certain city have certain opportunities to take advantage of smart cities. There are solutions that cover more than one city and village and there are solutions that cover only certain territories. With each such purpose-built system, there is also a circle of users who are able to use the system. As an illustrative example, we can take the system of electronic verification of electricity consumption.

The whole of Serbia can have access, but, of course, with certain personal data limitations. In order for a user to be generated and later to use the system, they need to expose their personal data to the threat that someone else finds out their personal information, such as information about the address of the household and the unique personal number in which the household is registered. All these data are kept in the same database. If someone were to get access to those databases, they would have a very large database of consumers throughout Serbia. Such systems and others that require the user to be identified using personal data must be very careful to protect the privacy of the data. The entire system is exposed, and used via a desktop/laptop computer, and also on smartphones and tablet devices. Keeping that data private is of great importance. Any leakage of information from their system may cause the privacy of its users to be compromised. The lack of seriousness in the understanding of privacy protection can lead to misuse of data. The next place is occupied by systems that are specific to cities, such as administrations that keep a database about companies, about taxes, about insurance, or bases connected to certain services.

In addition to the mentioned systems, which have been built and are planned for use, the infrastructures used for inspection and control of the city are also planned. These include various sensors, for example to turn on street lights, street cameras, traffic lights that are controlled and connected to the internet, and many other examples. They all generate a lot of data about people moving around the city, and in addition to digital traces, they also leave space for tracking individuals. It is important to note that any unauthorized use or abuse of these systems directly causes a threat to one's privacy. We refer the reader to [6] for more details on this topic.



Security

In addition to compromising privacy, it is also important to consider security. The security of a system guarantees us users, or observers, that we feel safer and that we are not afraid at all times that our privacy will be breached. The whole background of safety and security of smart cities is observed in a well-known principle. It could be said that the security of smart cities is only as strong as the weakest security component contained in the whole concept. In other words, regardless of the high-level security coverage, the architects of such systems must provide and map cases that are possible due to access to the system by external factors. One of the strategies to break into various systems used by practitioners is to bypass system security using security cameras.

Safety must be taken seriously, so that it is mapped so as not to allow many omissions in construction [7]. This proved practical when we look at the previous period. There have been a couple of intrusions of infrastructure systems by hackers into some of our infrastructure networks, state systems and also some cities were attacked, as well as in other countries [4]. If there is room for manipulation, there is an increasing chance that hackers will use it. One of the examples of such an attack is the used system component, which was subject to manipulation. They took advantage of the vulnerability of a component in the system and used it to make a background/undetected access, as well as to gain unauthorized access to some data. Another approach that was very significant is when the workers inside a company decided to connect to the network differently (by moving the LAN cables from the router to the connection in the company wall), so as to bypass the controlled network and expose the internal system to the outside world. It is for the same reason that human beings are often considered the weakest link. It is very important to hold security training in such important companies, in order to prevent steps that could threaten the data security of all citizens or citizens within a local community.

The digital divide

Weak points of smart cities can occur for various reasons, one of them being the digital divide [8], which can be present on several levels. It is not a division caused by direct selection, but by the possibility that exists in the current moment. As a parallel example, we can cite cities where the infrastructure is still expanding, so some have access to gas/sewerage, and some are still waiting for their part of the city to be built.

At the first level, the digital divide can refer to the lack of access to technologies and digital services among the population. This can create inequalities in access to information, education, health services and other key resources. These inequalities are also shown due to the territorial coverage of the city's infrastructure. Some parts of the city have more health facilities than others, so in one place patients will be able to choose which location they go to, while others will be forced to go to a specific facility and be on the waiting list for a much longer time.



At another level, the digital divide can refer to inequalities in the quality of digital infrastructure between different parts of the city. For example, some parts of the city may have faster and more stable internet access, while others may suffer from slower connections or even no access at all. This can happen with cable television, even though someone wants the services and to watch what's happening on some specific channels, but they don't have the opportunity due to infrastructural barriers. Due to geographical destinations, the signal of telecommunication operators also forces the use of a specific operator and does not give the possibility of choice.

Lack of digital literacy can also be a weak point, especially among the older population or among those less trained in the use of digital technologies. This can limit citizens' ability to take advantage of smart city solutions and services. Sometimes some services are available only through web presentations, but without knowledge about it or sufficient digital literacy and boldness to use the same, individuals are not able to take advantage of the good sides of the technology.

Let us take as an example the more frequent frauds that happen on the internet. Someone who is not trained well enough can compromise their privacy, even their security, if they share too much information on the internet. This is how they can suffer financially, send details that lead to additional charges for services at banks, mobile operators, and also pay for services they don't even use.

Addressing the digital divide requires comprehensive strategies that include improving access to technologies and digital services, infrastructure development, as well as education and awareness of digital tools and resources. These efforts can help build more inclusive and sustainable smart cities.

Dependence on technology

The concept of smart cities has attracted great minds, who organize competitions with smart city ideas called "Smart city challenge". There are various articles comparing their introduced innovations [9]. Do all these technologies help or harm?

By introducing new technologies into any aspect of our lives, we must be prepared to learn something new, to adapt to new details and to accept them. Is it a difficult step to perform? Is it a benefit to a certain city that there is automation of some process? This way of functioning of a city includes various other factors and how it will turn out later is not known in advance. In the article [10], smart works are mentioned as modern experiments.

Large projects in cities mostly require changes in infrastructure. In this aspect, this includes technological difficulties. To begin with, is it sustainable to develop and maintain a ready system. If it is subject to some vulnerabilities, it must be reacted quickly. In the later period, large unnoticed risks may appear due to the fact that introduced innovations or a new solution may bring unforeseen additional problems. In addition to all this, cities need to know



how to react to such problems in a timely manner, which can drain the budget, human resources, or it just happens that there are simply no capacities to cover these technological deficiencies. Projects in development fail due to wrong or insufficiently detailed planning, some such "I want to be a smart city" cities can fall victim to it.

Costs and financing

We have already touched on the question of financing in the previous part, but now we will go into a little more detail. As much as it is necessary to find qualified personnel for the construction of smart infrastructure, it is also necessary to determine in advance how much is needed or how much can be allocated financially. Some projects require even up to 50 million dollars [10]. Google has predicted more than 10 trillion US dollars in US cities by 2032. Justified or not, it does not change the fact that the price and costs are determined by how smart they want the solution to look, how much geographical area it must cover, whether there is already a stable connection that can be used or should create a new infrastructure for the same. The financing calculation can be evenly expanded due to territorial coverage, but it can also be exponentially increased if the requirements in the plans are too difficult to achieve.

The value of investments at the moment is expressed, at the world level, in billions, there are data from 2023 that say that the investment is worth over 190 billion. The period of covid dictated the introduction of new innovations around the world, and thus the breakthrough of large realizations of investments in smart cities jumped. When we look at the whole situation of progress, we can use a few words like super computer and artificial intelligence. Super computers would allow us to develop technology even faster, but certainly, the pace at which people can adapt to it will slow down. When we look at the prospect of artificial intelligence combining into smart cities, the current knowledge around artificial intelligence does not inspire confidence that we can let artificial intelligence make its way into everyday lives, even though the ultimate goal is to achieve such solutions. We believe that there are no experts who could, with a small deviation threshold, even estimate the costs and predict the financing planning for projects of this type.

Very interesting statistics [11] is covered and collected on the internet, we often come across contradictory data among various articles.

Regulation and standardization

At this stage of development, there is no industry standard or so-called best practice of what and how to introduce or perform processes in smart cities. It would not be difficult to draw a parallel in general and draw a conclusion from the IT sphere/area, but this still requires the engagement of experts who are capable of establishing the same.

Various open source tools can be applied, but maybe that's what brings privacy or data security into the system. Data collection must be developed in a transparent but secure



manner. This includes anonymization, data encryption and privacy protection [12]. In order to preserve compatibility between different systems that are connected, standards help us to connect these parts [13]. Systems often require specific setup even though their purpose of existence is universal. Concepts such as nature conservation, energy efficiency, waste management and transport are included through standards and regulations. All in all, they have to indicate and coordinate in accordance with the needs of the residents and the community.

Disaster resilience

This aspect seems like a not-so-important item, but in reality it is very important. Plans for the same can be different and mostly depend on territorial threats and risks of natural disasters [14]. Cities that are exposed to such risks must have a system that enables quick recovery and a subsystem that knows how to react in case the main system encounters problems. Let us just imagine situations when hard disk warehouses in Japan were destroyed due to the tsunami and the supply of them stagnated for a while, because the factory was not ready to return products in such cases. Smart cities can spread important information, so they must not allow a blockage or a major break of the smart city to happen [15]. They have to come up with a strategy that will be activated when some natural calamity or disaster is in progress, if only to save the data before it is lost forever.

Conclusion

We are facing an era in which we will witness great technological discoveries, but we must also be aware that some discoveries do not serve humanity positively. Smart city systems help us improve the quality of life, improve the efficiency of public services, manage resources more efficiently, and preserve our environment more successfully. Without the support of the smart city system, all urban environments would not be able to function and the entire city system would collapse.

It is very important to pay attention to the weak points of smart cities in order to avoid some risky situations when the entire system may break. The privacy of citizens, data security must be respected, the necessary expertise must be introduced with detailed planning, the standards of the IT sphere must be established and monitored, and the future of the same must be projected/planned. With a lot of attention and effort, all these necessary items can be done and complied with, and also prepared for future challenges.

New inventions have always been needed, this is how humanity has always been built and this is how nature and evolution dictate.

References

- [1] Mark Vallianatos, Uncovering the Early History of “Big Data” and the “Smart City” in Los Angeles, *Boom California*, 16. June 2015.



<https://boomcalifornia.org/2015/06/16/uncovering-the-early-history-of-big-data-and-the-smart-city-in-la/>

[2] Salah M. Alajeel, The History Of Smart Cities, The Los Angeles Tribune, 7. december 2020. <https://thelosangelestribune.com/2020/12/07/the-history-of-smart-cities/>

[3] Anwaar AlDairi and Lo'ai Tawalbeh (2017), Cyber Security Attacks on Smart Cities and Associated Mobile Technologies, Procedia Computer Science 109C (2017) 1086–1091, Uter and Informatino Systems, Makka, College of Computer and Informatino Systems, Makkah, Saudi Arabia. <https://www.sciencedirect.com/science/article/pii/S1877050917310669>

[4] Ismagilova, E., Hughes, L., Rana, N.P. *et al.* Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework (2022). <https://link.springer.com/article/10.1007/s10796-020-10044-1>

[5] R.W. LE MAITRE - Department of Geology, University of Melbourne, Melbourne, Parkville, Vic. 3052, Australia, *Numerical Petrology Volume 8*, (1982) 163-177. <https://www.sciencedirect.com/bookseries/developments-in-petrology/vol/8/suppl/C>

[6] Badouch, A., Krit, SE. (2022). Security and Privacy Issues in Smart City. In: Elhoseny, M., Yuan, X., Krit, Sd. (eds) Distributed Sensing and Intelligent Systems. Studies in Distributed Intelligence . Springer, Cham. https://link.springer.com/chapter/10.1007/978-3-030-64258-7_18

[7] Hadi Habibzadeh, Brian H. Nussbaum, Fazel Anjomshoa, Burak Kantarci, Tolga Soyata, A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities, 5. July 2019. <https://www.sciencedirect.com/science/article/abs/pii/S2210670718316883>

[8] Olga Kolotouchkina, Carmen Llorente Barroso, Juan Luis Manfredi Sánchez, Smart cities, the digital divide, and people with disabilities, April 2022. <https://www.sciencedirect.com/science/article/pii/S026427512200052X>

[9] Iulia-Cristina UȚĂ, Top 10 smart cities in the world, Brands minds blogs, April 2022.

https://brandminds.com/top-10-smart-cities-in-the-world/?gad_source=1&gclid=Cj0KCQiArrCvBhCNARIsAOkAGcVFHzwFkn5IV52-xln5B-IUXWgAheKSF_zSOog_kEivqpxfShuJz98aAhL5EALw_wcB

[10] Shannon Mattern, A City Is Not a Computer, Places Journal, February 2017. Accessed 03 Mar 2024. <https://placesjournal.org/article/a-city-is-not-a-computer/>



- [11] Barry Elad, Smart City Statistics 2023 By Companies, Market Share, Prioritized Areas and Country Rank, EnterpriseAppsToday blog. Accessed 03 Mar 2024. <https://www.enterpriseappstoday.com/stats/smart-city-statistics.html>
- [12] Ahmed Badran, Developing Smart Cities: Regulatory and Policy Implications for the State of Qatar, Dec 2021. <https://www.tandfonline.com/doi/citedby/10.1080/01900692.2021.2003811?scroll=top&needAccess=true>
- [13] Srikanth Chandrasekaran, How Standards Help Make Smart Cities a Reality, March 2021. <https://standards.ieee.org/beyond-standards/industry/technology-industry/how-standards-help-make-smart-cities-a-reality/>
- [14] Neha Bansal, Mahua Mukherjee, and Ajay Gairola, Smart Cities and Disaster Resilience, December 2017. https://www.researchgate.net/publication/312335316_Smart_Cities_and_Disaster_Resilience
- [15] Samarakkody A, Amaratunga D, Haigh R. Technological Innovations for Enhancing Disaster Resilience in Smart Cities: A Comprehensive Urban Scholar's Analysis. Sustainability, 2023. <https://www.mdpi.com/2071-1050/15/15/12036>