Journal of Infrastructure, Policy and Development 2024, 8(10), 8629.
https://doi.org/10.24294/jipd.v8i10.8629

Article

A comprehensive and in-depth study of the threats faced by smart cities and the countermeasures implemented in their key areas

Mehdi Houichi[1,*], Faouzi Jaidi[2,3], Adel Bouhoula[4]

[1] Higher School of Communication of Tunis (Sup'Com) LR18TIC01 Digital Security Research Lab, University of Carthage, Tunis 2083, Tunisia
[2] Higher School of Communication of Tunis (Sup'Com), Innov'Com Lab\Digital Security Research Lab, University of Carthage, Tunis 2083, Tunisia
[3] National School of Engineers of Carthage, University of Carthage, Tunis 2035, Tunisia
[4] Information Technology Department, Arabian Gulf University, Manama 329, Bahrain
*** Corresponding author:** Mehdi Houichi, mehdi.houichi@supcom.tn

CITATION

Houichi M, Jaidi F, Bouhoula A. (2024). A comprehensive and in-depth study of the threats faced by smart cities and the countermeasures implemented in their key areas. Journal of Infrastructure, Policy and Development. 8(10): 8629. https://doi.org/10.24294/jipd.v8i10.8629

ARTICLE INFO

Received: 15 August 2024
Accepted: 10 September 2024
Available online: 29 September 2024

Abstract: A smart city focuses on enhancing and interconnecting facilities and services through digital technology to offer convenient services for both people and businesses. The basic infrastructure of smart cities consists of modern technologies such as the Internet of Things (IoT), cloud computing and artificial intelligence. These urban areas utilize different networks, such as the Internet and IoT, to share real-time information, improving convenience for the inhabitants. However, the reliance of smart cities on modern technologies exposes them to a range of organized, diverse, and sophisticated cyber threats. Therefore, prioritizing cybersecurity awareness and implementing appropriate measures and solutions are essential to protect the privacy and security of citizens. This study aims to identify cyber threats and their impact on smart cities, as well as the methods and measures required for key areas such as smart government, smart healthcare, smart mobility, smart environment, smart economy, smart living, and smart people. Furthermore, this study seeks to evaluate previous research in this field, establish necessary policies to mitigate these threats, and propose an appropriate model for the infrastructure associated with IT networks in smart cities.

Keywords: smart city; digital technology; cybersecurity; privacy; Internet of Things

1. Introduction

A smart city embodies an urban landscape where modern digital technologies converge to enrich various facets of urban life for its inhabitants (Stratigea et al., 2015). Creating smart and sustainable infrastructure in cities depends on the development of information technologies (ICT), including the Internet of Things (IoT), sensors, artificial intelligence (AI), robotics, Web 4.0 technologies and smart grids Central to this concept is the utilization of ICT infrastructure to gather, analyze, and harness data for informed decision-making and streamlined service delivery (Gracias et al., 2023). These cities prioritize sustainability by optimizing resource utilization, reducing pollution, and advocating for eco-friendly practices (Sodiq et al., 2019). Embracing a citizen-centric approach, they actively involve residents and ensure accessible and responsive service provision. Collaboration among government entities, the private sector, academic institutions, and community stakeholders' fosters innovation, driving continual enhancement and adaptation to evolving urban challenges. As urbanization accelerates and the population increases, the significance of smart cities in tackling common urban challenges like congestion,

pollution, and infrastructure deficiencies grows (Shahidehpour et al., 2018). These cities serve as catalysts for economic growth, attracting investments, fostering entrepreneurship, and generating job opportunities. In line with the Sustainable Development Goals, smart cities actively contribute to sustainable development, resilience, and inclusive growth, thereby enhancing the overall quality of life. Many countries such as Dubai, Tokyo, Singapore, Hong Kong, Seoul, Helsinki, London and Riyadh, and India are currently making efforts to transform many cities into smart cities. It is especially worth noting that Saudi Arabia has invested up to 5 billion US dollars in the development of the new NEOM smart city (Satterthwaite, 2007). Riyadh, located in Saudi Arabia, is implementing anti-speeding traffic management measures, including the deployment of traffic control systems (ITS), including various devices and closed-circuit television (CCTV). Advanced analytics are employed to analyze traffic data historically, in real-time, and predictively, enabling the reporting of incidents and traffic conditions within the framework of traffic control units (Kim et al., 2023). Numerous emerging technologies are being integrated to streamline the evolution into smart cities, although their adoption also introduces inherent risks. A case in point is the deployment of sophisticated technologies like the Internet of Things (IoT) in smart homes, aimed at offering enhanced functionalities and convenience. Nevertheless, they also contain vulnerabilities that hackers can exploit to remotely control smart home systems. This experiment underscores the vulnerability of Z-Wave technology, commonly employed in smart home systems. In this instance, researchers demonstrated how an attacker could remotely open a smart door and disable the smart valve alert, thereby concealing a fire hazard within the house without the user's knowledge (Kim et al., 2020). While smart mobility offers residents of smart cities enhanced freedom of movement, it also presents a potential risk to life if exploited by attackers (Kim et al., 2021). During the Black Hat conference, researchers successfully showcased the remote hacking of an autonomous vehicle, leading to the forced activation of the brakes while in motion (Miller and Valasek, 2015). Hence, the targeting of a pivotal element within a smart city by a cyberattack could potentially lead to substantial harm to both individuals and assets. Notably, state-sponsored hackers leveraging advanced tools such as ransomware have emerged as significant threats to the integrity and security of smart cities (Ji-Young et al., 2019). Attacks targeting the fundamental infrastructure of smart cities not only serve the interests of cyber attackers but also benefit cybercriminals. By exploiting vulnerabilities in smart homes, cybercriminals can remotely control door locks or car key fobs to gain unauthorized access.

Moreover, the proliferation of the Internet of Things (IoT) exposes new vulnerabilities for intruders and other hostile actors to exploit. With billions of interconnected "things" deployed in smart cities worldwide, there exists a multitude of potential vulnerabilities and techniques that can be utilized (Sharma and Arya, 2023). Expanding on the aforementioned points, information security is paramount in smart cities to ensure heightened levels of confidentiality, availability, and integrity (Ismagilova et al., 2020). Additionally, it ensures the stability required by national services and organizations to maintain and improve livable intelligent environments. While smart cities aim to enhance productivity and efficiency,

neglecting cybersecurity could pose significant risks to residents and authorities. In summary, the primary security challenges faced by smart city environments are as follows:

A vast and intricate attack surface: As cities progress in sophistication, they will incorporate a larger array of systems and "systems of systems," amplifying the risk and consequences of potential attacks, thus necessitating improved control and visibility measures (Törngren and Grogan, 2018). Moreover, the integration of vendor solutions introduces complexity to intelligent city systems, particularly during periods of rapid technological advancement.

Insufficient supervision and organization: Complex systems will require stronger management and governance capabilities. Providing comprehensive updates to leadership about complex incidents will demand additional resources and capabilities.

In light of the ever-evolving cyber threats, researchers need to share info about risks and ways to prevent and respond to them. Smart cities offer big economic opportunities, but with more devices connecting, cyber attackers have more chances to strike. So, securing these cities means teamwork between local governments and businesses that rely on them. We also need to focus on identifying and protecting crucial assets, and setting up basic security rules to keep things running smoothly. Remember, a city's smartness is judged by how well it handles governance, transportation, environment, living conditions, healthcare, economy, and its people. It's crucial to ensure these areas meet minimum standards, quickly fix any problems, and keep private info safe from public networks

The structure of this paper is outlined as follows: In Section 2, we delve into foundational concepts pertinent to smart cities, including their benefits and architecture. Section 3 offers a comprehensive examination of the main threats, attacks, and countermeasures within the domains of smart city networks, elucidating their functionality and proposing effective solutions drawn from recent literature. Section 4 presents an analysis of cybersecurity threats in smart cities and corresponding countermeasures. Finally, Section 5 synthesizes the principal findings derived from our investigation, concluding with a discussion on potential avenues for future research.

2. Literature review of smart cities

The primary objective of constructing smart cities is to elevate the living standards of residents. To achieve this goal, a smart city optimizes its resources and establishes an intelligent ecosystem through digital technology. This encompasses the creation of inventive urban transportation systems, improvements to water supply and waste management infrastructure, and the adoption of more effective approaches for illuminating and heating buildings. Furthermore, it entails devising creative approaches to promote democracy and citizen participation in decision-making processes. Moreover, it involves guaranteeing a clean and secure environment, providing accessible public spaces, and offering user-friendly financial services that cater to the needs of the population without any restrictions or exclusions. It's

important to note that this integration is accomplished through the optimal utilization of ICT, transforming residents into smart citizens of a smart city.

2.1. Smart city applications

The rise of smart city technology has led to the development of sectors such as public services and traffic management, transportation, energy, water, healthcare and waste management. Smart cities integrate a wide range of Internet of Things (IoT) devices, from parking sensors and health monitoring to urban noise mapping, traffic control, route coordination and smart lighting (Angelidou et al., 2018). These sensors leverage IoT technology to operate seamlessly within the infrastructure of smart cities. Moreover, the cloud acts as a central hub for storing and processing data generated by smart city operations. Typically, smart city applications encompass various sections, as depicted in **Figure 1** which illustrates the core components of a smart city, which include smart governance, smart education, smart buildings, smart transportation, smart energy, and smart healthcare. Each of these components represents a key sector within a smart city that relies on advanced technologies and interconnected systems to improve urban living.

Figure 1. Smart city applications.

a. Smart government: Smart government requires the use of information and communication technology (ICT) to improve various aspects of public administration, including planning, management and operations (Houichi et al., 2021). Broadly speaking, it is about the integration of ICT at various levels of government for the purpose of providing effective information and better service to citizens. Smart government represents an evolution from traditional e-government practices towards more advanced and interconnected systems. By leveraging instantaneous data, smart government initiatives aim to improve situational awareness, enhance emergency response capabilities, reduce crime rates, and enhance overall municipal services (Dou et al., 2023).

b. Smart healthcare: Smart medicine involves the use of modern technologies such as wearable devices, Internet of Things (IoT), and mobile Internet to quickly access information (Amin and Hossain, 2020). It facilitates the seamless connection between individuals, healthcare facilities, and institutions, thereby enabling more efficient management of healthcare needs. These strategies include key entities such as doctors, patients, hospitals and medical research institutions. Smart healthcare; It covers a variety of dimensions, including disease prevention, patient monitoring, better diagnosis and treatment, better hospital management, healthcare decision-making, and advances in medical research. Remote monitoring is possible through a wireless network that connects smart devices to healthcare facilities and enables real-time data analysis (Dağtaş et al., 2008). The implementation process of smart healthcare within a smart city framework is depicted in **Figure 2**, which illustrates the flow of information between patients, healthcare centers, and caregivers, using various IoT devices such as sensors, cameras, GPS, Zigbee, Bluetooth, and others, all interconnected through the internet. The figure highlights how both formal and informal caregivers can monitor and manage patient health remotely, ensuring efficient and responsive healthcare delivery.

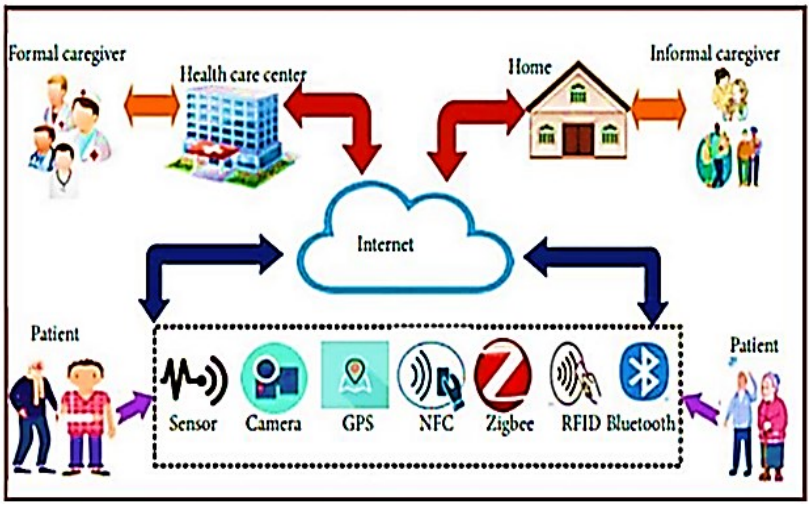

Figure 2. Smart healthcare concept (Zamel and Naif, 2023).

c. Smart energy: The existing energy grid infrastructure is struggling to keep up with the increasing demands of communities. There's a pressing need for a more reliable, scalable, manageable, environmentally friendly, and cost-effective energy production system, leading to the development of a smart and modern energy grid (Markovic et al., 2013). This advanced grid, empowered by information and communication technology, allows for bi-directional communication and flow of electricity among various grid components. It enables real-time monitoring, ensuring efficient power distribution between the grid and consumers. Moreover, it promotes the adoption of renewable energy sources, thus contributing to environmental sustainability.

d. Smart transportation: In contemporary traffic management systems, the objective is to optimize the utilization of existing infrastructure by integrating modern technologies. This integration seeks to boost network efficiency, ensure the

safety of vehicles and pedestrians, and minimize travel time. Meeting these goals entails deploying efficient transportation systems along with effective management protocols. Smart transportation systems provide various advantages, including the mitigation of traffic congestion, enhancement of safety measures, time-saving benefits, reduced fuel consumption, and overall improvement in service quality (Jeong et al., 2021). The main components of the system include the monitoring and recording system, weather information system, driver warning system, vehicle information system and automatic safety and police system for increased security. According to the ERSI definition, intelligent transportation systems are classified into four groups: practical measures to prevent road safety, location-based services, development of collaborative communication and global Internet services (Mun et al., 2009). Traffic Private networks play an important role in the efficient transportation system consisting of a high-speed vehicle network (Xia et al., 2021). The implementation process of smart transportation in a smart city is shown in **Figure 3**.

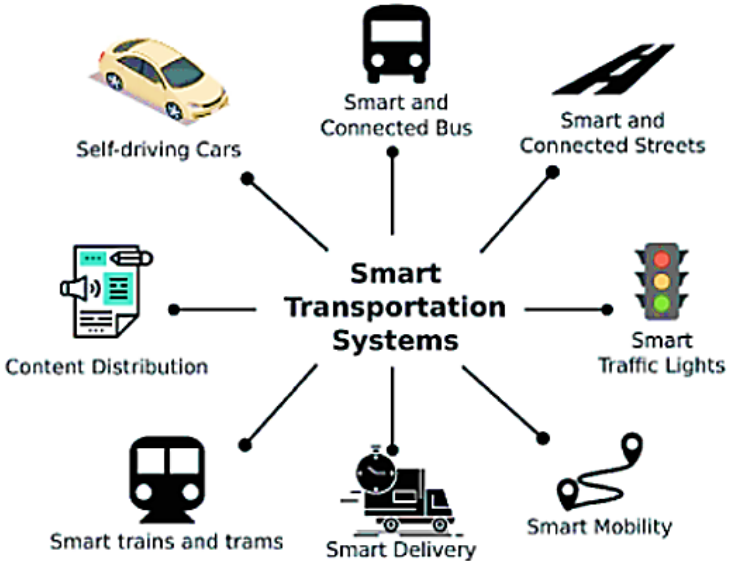

Figure 3. Smart transportation systems (Boukerche and Coutinho, 2019).

e. Smart building: Smart buildings employ a range of technologies including sensors and grid systems to enable communication among various building equipment (Jia et al., 2019). Additionally, they utilize smart meters to track energy consumption and transmit data to the smart grid. These buildings are designed to adjust their energy consumption according to the capabilities of the smart grid, while also allowing building owners to control equipment remotely. The interaction between smart buildings and the smart grid is essential to achieve the basic goals of the smart grid. This collaboration offers many benefits, including responsive feedback, better feedback, climax, and energy sharing. In general, the technical skills of construction consist of two main parts: construction technology and external technology.

In addition to the above-mentioned architectural features and functions of the smart city, factors such as smart economy, security, logistics, education and environment can also be included in the smart building process. **Figure 4** shows the

smart building and its components and illustrates the key components of a smart building, including sensors and actuators, networking and communication systems, software platforms, HVAC systems, and smart control devices (Silva et al., 2018).

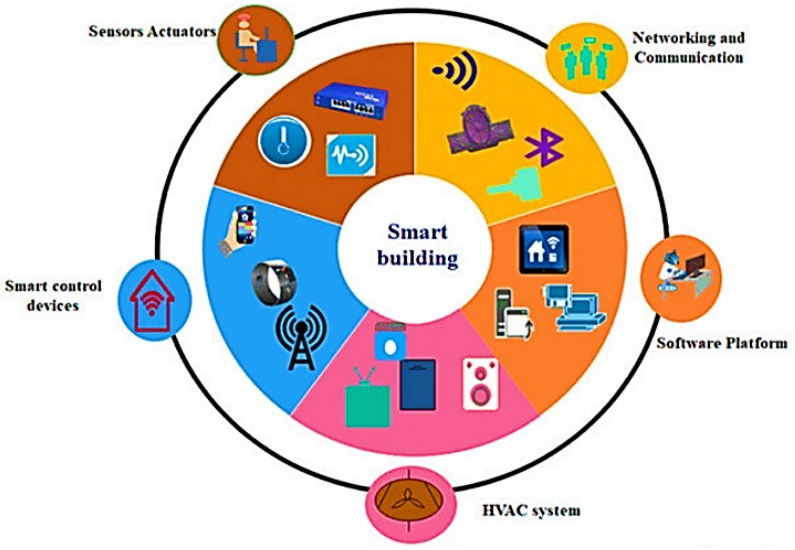

Figure 4. Smart building and its components (Zhuang et al., 2020).

f. Discussion: The progression of smart cities signifies a notable stride in improving the quality of life for urban dwellers. Smart cities aim to improve resource use, improve service delivery and promote sustainable development through the use of digital technologies and innovative solutions. The integration of various smart city activities emphasizes a holistic approach to achieving these goals. A key advantage of smart cities lies in the seamless integration of information and communication technologies (ICTs) across various sectors, resulting in more effective governance and service delivery. However, these advancements also bring forth challenges, particularly in the domain of cybersecurity.

As smart cities continue to expand their interconnectedness, they become increasingly vulnerable to cyber threats and attacks. The enormous amount of data generated and transmitted in the urban environment creates an attractive target for criminals looking to exploit security vulnerabilities. These concerns cover a wide range of issues, from data breaches to identity theft to disruptions in critical infrastructure and services. Additionally, the dependence on IoT devices and cloud computing creates additional opportunities for cyber-attacks and requires strong cybersecurity measures to protect private data and maintain the integrity of smart city operations. Concerns such as data privacy, network security, and combating cyber threats need to be comprehensively addressed to reduce risks and maintain public and stakeholder trust. As a result, while smart cities hold promise for improving the quality of urban life, they also pose serious cybersecurity challenges that require effective measures. By implementing strong security measures such as encryption, protocol authentication, and regular security assessments, smart cities can better manage risk and ensure their digital infrastructures thrive against cyber threats.

2.2. Smart city architecture

In order to thoroughly explore and grasp the concept of smart cities, it was essential to identify their foundational components. Through a comprehensive review of pertinent literature, we outlined the essential elements of smart cities, as depicted in **Figure 5**.

As illustrated in **Figure 5**, smart cities can be conceptualized within four distinct layers. Positioned at the top of this hierarchy is the provision of services and applications specifically designed for the inhabitants of smart cities. Below this uppermost layer are the technological infrastructure, network communication systems, and interconnected devices. Within the service and application layer, four primary subcategories emerged: smart transportation, smart communities, smart living, and smart environments.

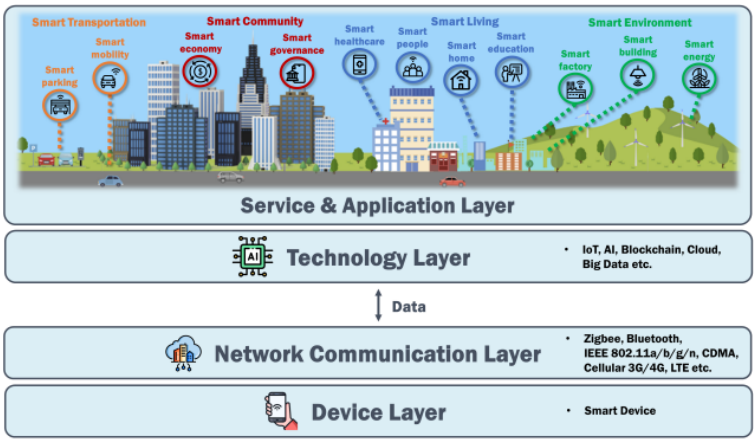

Figure 5. Smart city architecture.

Smart transportation encompasses aspects such as smart parking and intelligent mobility, while smart communities encompass domains like smart economy and efficient governance. Additionally, the domain of smart living can be further divided into key areas, including smart healthcare, smart individuals, smart residences, and smart education. Finally, the category of smart environments encompasses sectors such as smart factories, smart buildings, and intelligent energy management, each contributing significantly to the overall framework of a smart city.

a. Service and application layer: Smart city services and applications are designed with the overarching goal of enriching the lives of residents within these urban environments (Rehan, 2023). Leveraging advanced technologies, these services streamline access to urban amenities and utilities, ensuring efficient and convenient utilization. Within the realm of transportation, smart systems offer a diverse array of services, ranging from optimizing travel routes and sharing real-time traffic updates to facilitating car and bike-sharing programs, thereby enhancing the efficiency and accessibility of public transportation (Anwar and Oakil, 2023). Moreover, smart solutions address parking challenges by providing citizens with tools to identify available parking spaces swiftly. From a governmental standpoint, Information and Communication Technology (ICT) fosters transparency, community engagement, and effective crowd management, enabling swift responses to

emergency situations based on real-time public data (Van Hoang, 2024). Smart economy initiatives bolster labor market flexibility, regional productivity, and competitiveness, further enhancing the economic landscape. Smart living services empower residents to exchange real-time information, enabling them to address daily challenges efficiently while fostering connectivity within the community. Health and wellness are prioritized through remote monitoring and e-health services, delivering personalized medical care to citizens (Miranda et al., 2024). In the realm of home automation, smart systems empower users to remotely control IoT-enabled appliances, fostering convenience and energy efficiency (Putra et al., 2024). Additionally, urban infrastructure is optimized to enhance convenience, while educational systems embrace technology to offer flexible learning options. Environmental development is the mainstay of smart city initiatives, with digital energy management systems that facilitate time control and improve energy consumption and waste management. This dynamic approach promotes energy and environmental sustainability in smart city programs (La Barbera, 2023). However, many benefits provided by smart city technology also bring concerns about cyber security. The increase in attacks against city services highlight the need for strong security measures to protect the system and maintain public safety. To effectively deal with emerging threats on the internet, police strategies need to change with a strong emphasis on data analytics in future police operations (Ahmad et al., 2024).

b. Technology Layer: In addressing diverse challenges within smart cities, cutting-edge technologies play crucial roles by leveraging the abundance of generated data in efficient and secure ways. At the forefront is the Internet of Things (IoT), which forms the basis for the development of urban infrastructure by connecting various ICT tools and offering new solutions (Egbert and Leese, 2021). Research projects have investigated the use of IoT technologies in different areas of the smart city, including pollution management (Syed et al., 2021). Infrastructure and cloud are examples of smart cities where data fragmentation has become a major problem (De Nicola and Villani, 2021). Real-time data collection is enabled by sensors in IoT devices such as RFID, infrared (IR), GPS, and laser scanners that are fed into the cloud or storage, allowing remote control and management of devices (Houichi et al., 2022). Artificial Intelligence (AI) is rapidly evolving to provide complex services swiftly and efficiently, catering to both small-scale elements like smart homes and large-scale infrastructure such as smart transportation (Raj et al., 2022). Big data technology serves as a cornerstone for AI, facilitating the collection and analysis of vast datasets generated in smart cities, empowering AI to make informed decisions and predictions. Furthermore, blockchain and deep learning technologies hold promise for enhancing automation services, allowing for autonomous data learning and decision-making (Liu et al., 2020). Authentication technology, viewed through a blockchain lens, is also under scrutiny for smart city applications (Rejeb et al., 2021). Yet, privacy and security concerns pose significant challenges as data traverses various sectors within smart cities. Blockchain seems to be a possible solution that provides autonomy through smart contracts and decentralized management, increasing the security of smart city operations (Waseem et al., 2023). Additionally, cybersecurity research is being conducted to address issues related to augmented reality (AR) technology in the smart city (Böhm et al.,

2021). Perception of smart city technology depends on factors such as your experience, data privacy and security. When tangible benefits, such as good public services, are clearly visible, users are more likely to discover good smart city applications.

c. Network communication layer: Networking is a pillar of smart cities and facilitates seamless interaction of different activities and services. Applications necessitating short-range communication, such as smart grids, water services, and energy-efficient buildings, typically leverage IEEE 802.15.4 (Zigbee), offering longevity with minimal energy consumption. Alternatively, IEEE 802.15.1 (Bluetooth) can serve similar purposes, ensuring efficient communication (Zanaj et al., 2021). For broader coverage and higher data rates, protocols like IEEE 802.11a/b/g/n find widespread use across smart city systems. The latest iteration, IEEE 802.11n, operates across 2.4 and 5.1 GHz bands, employing advanced techniques like OFDM and DSSS to enhance performance. Moreover, it facilitates reservation-based operations through PCFs and best-effort operations via DCFs, catering to diverse data traffic requirements, including real-time multimedia (Chandramouli et al., 2019). In scenarios requiring cellular connectivity, 3G and 4G protocols prove instrumental, offering packet switching for data and voice communication. LTE, an advanced cellular technology, ensures global coverage through roaming capabilities. Additionally, satellite communications are used in applications such as UAVs, network monitoring and people transportation. It uses frequencies of 1.53 and 31 GHz and uses TDMA and FDMA in the data link for continuous transmission (Routray and Mohanty, 2021). Narrow-band technologies emerge as efficient solutions for supporting numerous IoT devices within smart city infrastructures, including grids and meters. However, despite their efficacy, security remains a concern, rendering them vulnerable to cyber threats. To address this, ICN routers are proposed for smart home networks, offering enhanced content distribution and cybersecurity through increased caching capacities (Pruthvi et al., 2023). Protecting wireless sensor networks (WSNs) within smart cities is paramount, prompting research into anomaly detection technology and the development of attack classification frameworks (Kanellopoulos et al., 2023a). These endeavors underscore the critical importance of cybersecurity in safeguarding the integrity and functionality of smart city networks.

d. Device and sensor layer: Devices and sensors are essential parts of smart cities, enabling the integration of smart devices embedded in sensors and motors. These tools play an important role in measuring, collecting and managing various data (Kanellopoulos et al., 2023b). Data pertaining to citizen activities, parking availability, and environmental conditions like light, noise, temperature, and humidity are seamlessly gathered through IoT sensors and amalgamated via ICT infrastructure (Rajendran et al., 2022). Citizens interface with this wealth of data through tangible devices such as wearables and smartphones, enabling visual access and control. Concurrently, equipped facilities leverage IoT sensors to monitor and analyze real-time data, tailoring their responses to specific needs and objectives. The emergence of smart city sensing heralds a transformative shift towards more intelligent urban services, with extensive research exploring its current and historical implications (Mortaheb and Jankowski, 2023. Despite the unparalleled connectivity

afforded by the widespread adoption of IoT devices, concerns persist regarding the security of end-node devices. This heightened connectivity, while enabling advanced services, necessitates a renewed focus on confidentiality and security measures to mitigate potential vulnerabilities and safeguard interconnected smart devices (James and Rabbi, 2023).

e. Discussion: The breakdown of smart city infrastructure into distinct layers offers a comprehensive framework for understanding the complex nature of these urban environments. At the heart of smart cities are intricate networks of interconnected devices and sensors, facilitating the seamless collection, analysis, and utilization of vast data sets. This infrastructure supports a diverse range of services and applications aimed at improving residents' quality of life while promoting sustainability and efficiency across various sectors. The utilization of Information and Communication Technology (ICT) forms the backbone of smart city initiatives, enabling real-time data exchange, automation, and connectivity. However, the widespread integration of ICT also brings significant cybersecurity challenges. As smart cities rely more on interconnected digital systems, they become increasingly vulnerable to cyber threats and attacks. Malicious actors may exploit vulnerabilities in smart city infrastructure to gain unauthorized access, disrupt services, or compromise sensitive data, posing risks to citizen safety and privacy. The extensive deployment of IoT devices, cloud platforms, artificial intelligence, and big data analytics within smart city environments creates numerous entry points for cyberattacks. While these technologies offer significant benefits in terms of efficiency and innovation, they also introduce new avenues for exploitation if not adequately secured. Concerns such as data privacy, network security, and resilience against cyber threats must be addressed proactively to safeguard smart city infrastructure and maintain public trust. Moreover, the interconnected nature of smart city systems complicates cybersecurity efforts, necessitating a holistic approach to risk management and mitigation. Policymakers, urban planners, and cybersecurity professionals must collaborate to develop robust cybersecurity strategies tailored to the unique challenges posed by smart city environments. This may involve implementing encryption protocols, authentication mechanisms, and intrusion detection systems to detect and thwart cyber threats in real-time.

In conclusion, while ICT plays a crucial role in driving the advancement of smart cities, it also introduces inherent cybersecurity risks that must be effectively addressed. By prioritizing cybersecurity awareness, investing in resilient infrastructure, and fostering collaboration between stakeholders, smart cities can mitigate risks and ensure the continued safety, security, and sustainability of urban environments in the digital age.

3. Advances in smart city security

3.1. Literature review

In recent years, the significance of cybersecurity threats in the digital realm has become increasingly apparent, evidenced by numerous incidents directly impacting the security of nations and individuals (Khan, 2023). The evolution of digital

technologies and cyberspace has not only revolutionized the way tasks are accomplished, but it has also reshaped power dynamics on national and international scales (Valencia Rojas, 2023). This shift in paradigm emphasizes the vital importance of information systems, digital communication, and the wider digital landscape in enabling well-informed decision-making processes. While we now possess the capability to generate and manage vast amounts of information, the security of this data has never been more precarious. To ensure the sustainability and competitiveness of global infrastructures, significant investments have been directed towards fortifying digital resources against security threats (Krishna et al., 2023). Hassan et al (Hassan et al., 2024). highlight the interconnected nature of the modern world, emphasizing the imperative of safeguarding information systems, both public and private, to support organizational activities and maintain consumer trust. Indeed, as noted by Marin et al., organizations demonstrating a robust commitment to information security can foster enduring relationships with customers, a crucial aspect also underscored in the context of smart city adoption (Marín Díaz et al., 2023). Information security encompasses diverse domains, primarily focusing on safeguarding data and information from unauthorized access, misuse, or alteration. Ensuring confidentiality is paramount, particularly concerning sensitive data such as personal or financial information, to mitigate risks of identity theft or reputational damage. Furthermore, maintaining data integrity is essential to preserve accuracy and reliability, preventing erroneous decisions or process errors (Duggineni, 2023). Conversely, guaranteeing data availability is imperative to mitigate disruptions caused by technical failures, cyber-attacks, or natural disasters, as underscored al (Tahmasebi, 2024). Within the context of smart cities, the repercussions of compromised data availability extend beyond inconvenience, impacting various facets of urban life, including citizen welfare, economic stability, and public safety. Thus, prioritizing robust information security measures is indispensable to safeguarding the integrity and functionality of smart city infrastructures and ensuring their resilience in the face of evolving cyber threats (Ahmad et al., 2024b). The intersection of information security, information science and technology creates a complex and interconnected environment. At the heart of this environment is data science, an interdisciplinary field focused on extracting knowledge and insight from data using techniques such as collection, cleaning, analysis, visualization and modelling. Technology serves as a basis for information security and information science, allowing them to be developed and integrated into modern infrastructure (Adeleye et al., 2024). Technological advances have led to the growth of digital data and the development of advanced tools and algorithms to process and analyze data effectively. Key technologies that support information security and information science include big data networking, cloud computing, artificial intelligence (AI), machine learning (ML), image encryption, and networking and communications (Siripurapu et al., 2023). As Varghese (Varghese, 2024). highlights, the cloud has become a transformative force in organizations, revolutionizing data storage, accessibility, and processing capabilities. Cloud services offer scalable infrastructure capable of accommodating vast datasets and hosting data science applications and security solutions. Cloud providers maintain extensive data centers equipped with diverse resources, enabling dynamic allocation and reallocation of computing

resources based on demand. Elasticity is a hallmark feature of cloud platforms, allowing for automatic adjustment of resources to meet fluctuating workloads. This flexibility allows users to scale resources up or down as needed without being constrained by physical hardware investments. Additionally, dynamic scaling ensures efficient resource utilization and cost-effectiveness (Kavitha et al., 2023). The convergence of cloud computing and machine learning offers unparalleled opportunities for scalable and flexible solutions in processing, analyzing, and deploying AI-powered applications. Integrating machine learning with cloud computing infrastructure facilitates the training of complex models and the processing of large datasets (Li et al., 2024). ICT plays an important role in the creation of smart cities that integrate infrastructure, architecture, objects and people to improve and solve social, economic and environmental problems. Technologies such as cloud computing, big data analytics, artificial intelligence (AI), blockchain and Internet of Things (IoT) form the basis of smart city initiatives. Security in smart cities is considered a dynamic concept that includes both digital and physical components to protect directly and indirectly. Security as a critical factor influences technology acceptance, emphasizing its multifaceted nature that extends beyond technical considerations to encompass subjective perceptions and human behavior. The adoption of emerging technologies in smart cities fuels innovation and underpins the development of smart environments, governance, and economies (Nastjuk et al., 2022). Indeed, technology and innovation are integral to the fabric of smart cities, distinguishing them from traditional urban centers. However, dependence on advanced technology and a high degree of interoperability make smart cities vulnerable to technological overload. Protecting infrastructure, systems, and data from malicious activity is critical to the security, privacy, and reliability of smart city services. Therefore, it is urgent to find and implement effective mitigation strategies to address these problems. It is important to note that, although the security and privacy issues facing smart cities are not entirely new, they are intensified in relation to the nature of urban environments (Rizi and Seno, 2022). The proliferation of thousands of devices and applications aimed at enhancing processes and citizen well-being introduces vulnerabilities related to security and privacy. The risks associated with smart systems driven by artificial intelligence, which not only collect sensitive information but also wield control over city infrastructure, influence the lives of citizens (Zamponi and Barbierato, 2022). Empirical studies, including European projects, acknowledge the inherent challenges posed by big data, data analytics, artificial intelligence, and machine learning in the context of smart city development (Bibri et al., 2023). Security embodies a dynamic concept, characterized by proactive measures aimed at averting harm through digital and physical avenues, encompassing both direct and indirect threats. In the context of smart cities, security is a holistic concern, addressing all facets of urban life and permeating every aspect of its infrastructure. Thus, safety in smart cities transcends mere technical parameters, intertwining with human behavior and subjective experiences (Houichi et al., 2023). Cybersecurity is critical to protecting critical infrastructure, systems and resources that play a vital role in the lives and well-being of communities. Electricity-using infrastructures, transportation networks, water treatment plants, communication systems and more need to be fully protected against

cyber threats to prevent outages, unauthorized access or destruction and possible damage to the city. Therefore, cybersecurity considerations, including adherence to best security practices, critical risk assessment, and establishment of appropriate controls, should be integrated into the design and planning of critical infrastructure from the outset (Nurthen, 2023).

In conclusion, the discourse on cybersecurity within the context of smart cities underscores the growing significance of safeguarding digital infrastructures against evolving threats. The digital transformation of urban environments has revolutionized societal processes and economic landscapes, necessitating robust security measures to protect critical data and infrastructure. We have explored the multifaceted nature of cybersecurity, encompassing aspects of information security, data integrity, and system availability. Moreover, the convergence of technology, data science, and innovation has paved the way for scalable solutions in addressing cybersecurity challenges, particularly in the domains of cloud computing, artificial intelligence, and machine learning. Our review has highlighted the intricate interplay between technological advancements, governance frameworks, and societal perceptions in shaping the security landscape of smart cities. The dynamic nature of cybersecurity demands proactive measures and continuous adaptation to mitigate risks and vulnerabilities. As we move forward, it is imperative to delve deeper into existing research and solutions in this domain, examining their efficacy and relevance in real-world smart city deployments. By studying the diverse works and solutions implemented thus far, we can glean valuable insights and best practices to inform future strategies for enhancing cybersecurity resilience in smart urban environments.

3.2. Existent solutions for cybersecurity in smart city

In this section, we embark on an analytical exploration of existing research and solutions tailored to fortifying the security infrastructure of smart cities. Our approach is anchored in the utilization of prior studies and initiatives, serving as a foundation for our analytical endeavors. As we delve into this investigation, our aim is to leverage the insights and findings from previous research to inform and enrich our own methodologies and conclusions, particularly focusing on existing solutions developed by researchers. Several security and privacy solutions have been introduced and are actively employed to address the pressing threats concerning security and privacy within smart environments as illustrated in **Figure 6**.

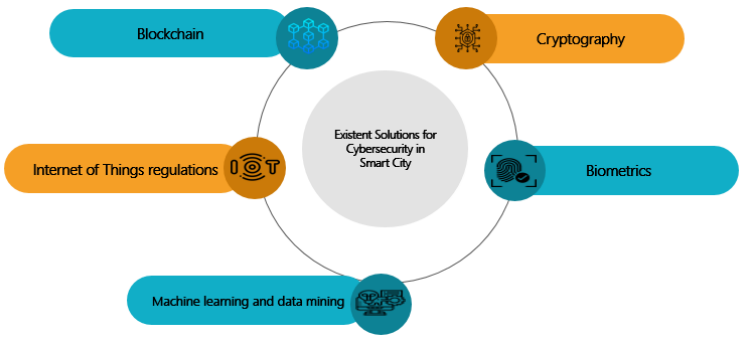

Figure 6. Solutions for cybersecurity in smart city.

a. Blockchain: Blockchain technology stands as a transformative force, offering decentralized and distributed solutions crucial for the advancement of smart cities. This peer-to-peer technique serves as a cornerstone for securely storing transactions, agreements, and contracts across myriad computers, fundamentally reshaping how data is managed within urban environments. Originally conceived for cryptocurrencies like bitcoin and litecoin, blockchain has swiftly evolved to become a linchpin in the pursuit of robust cybersecurity and privacy in smart city infrastructures. Its decentralized architecture, highlighted in a comprehensive survey by Singh et al., underscores its indispensability in fostering trust and reliability within IoT ecosystems crucial for smart city development (Singh et al., 2023). The decentralized nature of blockchain technology not only facilitates secure and transparent communication among interconnected devices but also empowers diverse applications to operate in a distributed manner. Pioneering research, exemplified by Beng and Zhu blockchain-based security framework for smart cities, showcases its pivotal role in fortifying communication networks and enhancing system resilience (Meng and Zhu, 2024). Moreover, blockchain's integration into various domains, including vehicular communications, personal data management, and cloud-based applications, underscores its versatility and adaptability in addressing multifaceted cybersecurity challenges prevalent in smart urban environments. Furthermore, El Majdoubi et al.'s blockchain-based access controls provide a robust framework for data owners to manage access rights securely, ensuring the preservation of users' privacy in smart city ecosystems (El Majdoubi et al., 2020). In essence, blockchain technology emerges as a linchpin in the quest to fortify cybersecurity and privacy in smart cities. Its transformative potential extends far beyond traditional applications, offering scalable and decentralized solutions essential for building resilient and secure urban environments capable of withstanding evolving cyber threats. Through its innovative capabilities, blockchain promises to revolutionize the landscape of smart city development, fostering trust, reliability, and resilience in the digital age (Singh et al., 2020).

b. Cryptography: Algorithms employing cryptography techniques serve as the bedrock for safeguarding security and privacy within information-centric smart city applications, ensuring that unauthorized parties are barred from accessing data during storage, transmission, and processing. This section explores the existing cryptographic tools used in smart city applications. Traditional encryption algorithms and standards, despite their robustness, often fall short for resource-constrained smart devices due to high energy consumption and computational demands (Singh et al., 2021). Consequently, there is a crucial need for lightweight encryption methods suitable for practical cryptographic algorithm implementations. For example, (Azzedin, 2023) proposed a mechanism designed for IoT-based scenarios that enhances end-to-end communication security by protecting against distributed Denial of Service (DoS) attacks. Similarly, (Lansky et al., 2022) developed a lightweight authentication protocol leveraging public key encryption strategies to fortify security in smart city applications. Moreover, the emergence of homomorphic encryption has garnered significant attention owing to its prowess in performing computations on encrypted data (Nguyen et al., 2024). This technique is especially crucial in the evolving landscape of data processing within cloud environments,

where data needs to be processed without decryption to maintain its security. Homomorphic encryption enables computations on encrypted data without exposing it, ensuring that privacy and security are preserved even during processing. This encryption technique finds utility in diverse domains, ranging from safeguarding electricity consumption in Smart Grid (SG) systems to addressing security and privacy concerns in cloud computing and healthcare monitoring systems. Furthermore, cryptographic approaches play a pivotal role in enhancing security and privacy in cloud-based data storage environments, significantly bolstering data security, especially in public cloud environments. These techniques also lend support to well-established privacy preservation algorithms, enabling precise analysis results. However, it's imperative to acknowledge the susceptibility of cryptographic algorithms to attacks, such as simple power analysis, which can manipulate data integrity and device performance. Consequently, rigorous research into cryptographic algorithms is essential to ensure data security and privacy. Additionally, cryptography offers viable solutions for addressing privacy leakage stemming from public access policies (Yang et al., 2020).

c. Biometrics: Biometrics serve as a prevalent method for authentication within IoT-based infrastructures, relying on human behavioral traits to automatically identify individuals using bio-data extracted from various sources such as faces, fingerprints, signatures, and voices (Silasai and Khowfa, 2020). Among these methods, brainwave-based authentication stands out for its remarkable accuracy and efficiency (Sooriyaarachchi et al., 2020). Panda et al. proposed a mutual authentication protocol to safeguard user privacy in storage devices effectively (Panda and Chattopadhyay, 2020). However, it is crucial to acknowledge the heightened risk of privacy breaches if biometric approaches are not implemented correctly (Yang et al., 2021). Furthermore, the potential of biometrics extends beyond authentication, with promising applications in diverse fields such as e-business. In the realm of cybersecurity, biometrics can also play a pivotal role in securing communication channels, as demonstrated by Rahman et al. Their study proposed a cost-effective safety mechanism based on biometrics for unmanned aerial vehicles (UAVs) to detect and respond to cyberattacks effectively (Rahman et al., 2024). This approach showcases the versatility of biometrics in addressing cybersecurity challenges across various scenarios, emphasizing its potential significance in ensuring the security and integrity of IoT-based systems.

d. Machine learning and data mining: Machine learning, a subset of artificial intelligence, focuses on developing systems capable of learning from past experiences. In the realm of smart cities, machine learning techniques offer significant potential for enhancing various aspects of the smart city ecosystem, including cybersecurity, traffic management, resource allocation, and more. Specifically, in cybersecurity, machine learning techniques present promising opportunities to enhance the efficiency of intrusion detection systems in IoT environments, which are integral to smart cities. Wireless Sensor Networks (WSNs) play a crucial role in monitoring and managing urban infrastructures. For instance, Ahmad et al. demonstrated the benefits of using machine learning technologies to improve security in Wireless Sensor Networks (WSNs) (Ahmad et al., 2022). Similarly, Bakshi et al. pioneered a machine-based approach to strengthen data

sensing security in WSNs (Bakshi and Sahu, 2022). Additionally, AlQahtani et al. created a novel model utilizing machine learning algorithms to effectively detect attacks in Wi-Fi networks (AlQahtani et al., 2024). Moreover, machine learning technologies have been crucial in bolstering defense strategies against intrusions. Belavagi et al. developed a model that integrates game theory and machine learning to detect and prevent intrusions in WSNs, highlighting the synergy between these fields in cybersecurity (Belavagi and Muniyal, 2021).

Beyond cybersecurity, machine learning can be employed in predictive maintenance of urban infrastructure, optimizing energy consumption in smart grids, and enhancing public safety through real-time surveillance systems. Various machine learning techniques, including supervised and unsupervised learning, show promise in identifying the presence of botnets. However, challenges such as real-time monitoring and adaptability to new attacks persist in machine learning-based detection methods, emphasizing the need for continuous innovation and research.

Data mining offers another approach for managing security and privacy concerns in smart city environments. Lofgran et al. illustrated how vast datasets collected by sensors in smart cities can be utilized to extract valuable insights and regulations, thereby enhancing service delivery (Löfgren and Webster, 2020). Nevertheless, the use of data mining techniques raises concerns about the potential disclosure of sensitive user information, such as location data. To address this issue, privacy-preserving data mining techniques can be employed to protect user privacy while still deriving actionable insights from collected data, ensuring that smart city initiatives remain secure and privacy-conscious.

e. Internet of Things regulations: The Internet of Things (IoT) encompasses a diverse range of communication technologies, including machine-to-machine communication, sensors, wireless communication, and radio frequency identification. Despite its rapid expansion, the IoT industry currently lacks comprehensive regulation, resulting in significant security and privacy concerns (Karale, 2021). The widespread use of unsecured smart devices across various sectors, such as military and healthcare, combined with the susceptibility of IoT devices to hacking, has led to the emergence of new cyberattacks exploiting vulnerabilities across all layers of the IoT protocol stack. Although the IoT industry has long been aware of these security and privacy challenges, recent cyberattacks on IoT devices have heightened the awareness of the critical need for robust security measures and regulatory frameworks (Ahmed and Khan, 2023). These attacks have served as a catalyst, highlighting the imperative for implementing stringent security mechanisms and regulations to safeguard internet-connected devices effectively.

f. Discussion: In this section, we conducted an in-depth analysis of existing research and solutions aimed at bolstering the security infrastructure of smart cities. Through the examination of prior studies and initiatives, we aimed to glean insights and enrich our own methodologies and conclusions, with a particular focus on solutions developed by researchers. Our exploration covered several key areas, including blockchain technology, cryptography, biometrics, machine learning, data mining, and IoT regulations. We found that blockchain technology stands out as a transformative force in enhancing cybersecurity and privacy within smart cities. With its decentralized architecture and versatility, blockchain offers scalable and

distributed solutions crucial for building resilient urban environments. Cryptography techniques play a pivotal role in safeguarding data integrity and confidentiality, albeit with challenges such as energy consumption and susceptibility to attacks. Biometrics offer promising authentication methods, with applications extending beyond traditional authentication to areas such as e-business and UAV security. Machine learning and data mining techniques present opportunities for enhancing intrusion detection systems and extracting valuable insights from sensor data. However, challenges such as real-time monitoring and privacy concerns necessitate further research and development. Additionally, the lack of comprehensive regulations governing IoT devices underscores the urgent need for robust security measures and regulatory frameworks to safeguard internet-connected devices effectively. Overall, while significant research efforts have been devoted to enhancing the security of smart cities, continued evolution and improvement of stakeholders and technical solutions are imperative. Collaborative efforts among researchers, policymakers, and industry stakeholders are essential to address emerging cybersecurity challenges and ensure the resilience and security of smart city infrastructures in the face of evolving threats.

4. Analysis of cybersecurity threats in smart cities and corresponding countermeasures

4.1. Cybersecurity risks in smart cities

Cybersecurity risks within smart cities are multifaceted and diverse, owing to the wide array of technologies and interconnected systems present. In this section, we delve into a comprehensive analysis of these risks, drawing insights from extensive research in the field. By identifying and understanding the various threats, we can develop effective countermeasures to fortify the security infrastructure of smart cities. Through our analysis, we have categorized cybersecurity risks in smart cities into distinct domains, each presenting unique challenges and vulnerabilities. Through our analysis, we have categorized cybersecurity risks in smart cities into distinct domains, each presenting unique challenges and vulnerabilities. These domains include access control, which encompasses threats related to unauthorized access to sensitive systems and data, posing risks to confidentiality and integrity. Network vulnerabilities arise from weaknesses in network infrastructure, such as vulnerabilities in communication protocols and data transmission mechanisms. Data privacy concerns revolve around the protection of personal and sensitive information, safeguarding against unauthorized disclosure or misuse. Vulnerabilities associated with Internet of Things (IoT) devices, including insecure configurations, lack of encryption, and susceptibility to remote attacks, constitute another significant domain. Infrastructure vulnerabilities arise from weaknesses in physical systems, including power grids, transportation networks, and communication systems.

Challenges related to human factors, such as user negligence, social engineering attacks, and insider threats, are attributed to human behavior.

Additionally, issues concerning the absence of standardized security protocols and regulations contribute to inconsistencies and gaps in cybersecurity frameworks,

forming the domain of security standards and regulation. Our analysis employs a structured framework to systematically examine each domain of cybersecurity risk within smart cities.

By delineating the specific threats and vulnerabilities within each category, we gain deeper insights into the underlying challenges and potential impact on urban environments. the analysis underscores the critical importance of addressing cybersecurity threats in smart cities comprehensively. By understanding the diverse nature of these risks and their implications across different domains, stakeholders can implement targeted countermeasures to mitigate vulnerabilities and enhance the resilience of urban infrastructures. The detailed classification of risks presented in **Figure 7** serves as a valuable reference for policymakers, urban planners, and cybersecurity professionals in devising effective strategies to protect smart cities against evolving cyber threats.

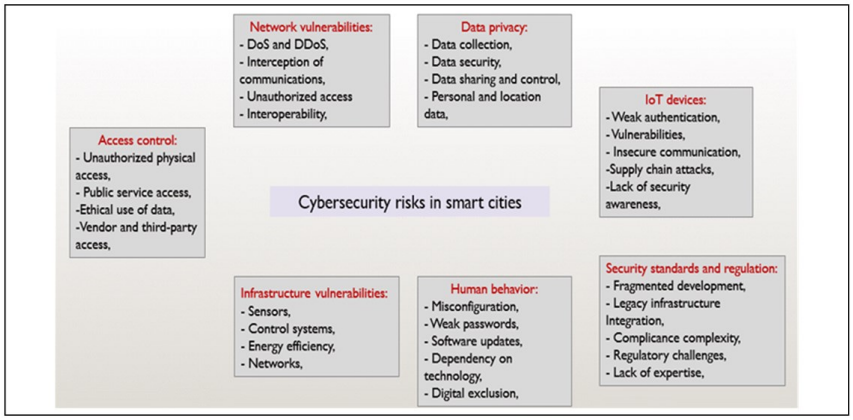

Figure 7. Map of cybersecurity risks in smart city.

a. Access control deficiencies: Access control is a critical domain within the realm of cybersecurity, especially in the context of smart cities, where the interconnectedness of various systems and devices creates vulnerabilities that could be exploited by malicious actors (Demertzi et al., 2023). One significant risk is unauthorized physical access, where individuals gain physical access to critical infrastructure or devices, potentially compromising their security. In a smart city environment, this could lead to disruptions in essential services or even endanger public safety (Petrova and Tairov, 2022). Additionally, the access control mechanisms for public services need to be robust to prevent unauthorized individuals from accessing sensitive data or resources, safeguarding the privacy and security of citizens. Using good behavior is another important aspect of managing smart cities. With the large amount of data provided by sensors and related devices, the problem of misuse or ineffective access to this data arises, leading to privacy violations or other illegal activities (Jaïdi et al., 2018). Effective controls are needed to ensure that data is used accurately and in accordance with legal guidelines. Retailers and third parties pose another major security challenge in smart cities. Many smart city projects are dependent on third-party suppliers for various services and technologies, increasing the risk of security breaches or data leaks if appropriate controls are not in place (Telo, 2023). It is essential to vet and monitor third-party access carefully,

implementing robust access control measures to mitigate these risks effectively. Research in the domain of access control in smart cities has focused on developing advanced authentication and authorization mechanisms to enhance security. Kalunga et al. use a biometric authentication method to strengthen access control for critical infrastructure and public services (Kalunga et al., 2020). Additionally, Ghorbel et al. use blockchain technology to create tamper-proof access logs and audit trails, improving transparency and accountability in access control processes (Ghorbel et al., 2022). Furthermore, research has emphasized the importance of adopting a comprehensive approach to access control, considering both technical and organizational factors. This includes establishing effective access management policies and procedures, conducting regular security audits and assessments, and providing ongoing training and awareness to staff and stakeholders. Overall, addressing cybersecurity issues in access management is essential to ensure the integrity, confidentiality, and availability of information and services in smart cities. By leveraging research-driven solutions and adopting best practices in access control management, smart city stakeholders can strengthen their cybersecurity posture and build trust among citizens and partners. Securing the access to sensitive data and services in critical infrastructures as a main objective is a great challenge for deploying secure smart cities that requires setting up trusted security policies (Remotti, 2021). while security solutions have to remain compliant and regularly updated to follow and track the evolution of security threats (Xia et al., 2023). To improve access control in urban environments, it is important to adopt a comprehensive approach that includes access detection, authentication and authorization, secure resource management, and performance-based auditing. Firstly, deploying robust intrusion detection systems allows for the timely detection of unauthorized access attempts or suspicious activities, enabling quick response and mitigation. Second, implementing strong authentication and authorization processes reduces the risk of unauthorized access by ensuring that only authorized users have access to systems and private data. Thirdly, practicing secure device management helps ensure that IoT devices are properly configured, updated, and monitored to prevent potential vulnerabilities and unauthorized access points. Finally, using role-based controls provides better control of user rights and permissions, ensuring that people only access the tools necessary for their role. By integrating these mitigation strategies, smart cities can significantly enhance their access control mechanisms and bolster overall cybersecurity posture.

b. Infrastructure vulnerabilities: Infrastructure vulnerabilities represent a significant cybersecurity concern in smart cities, as they encompass various components essential for the functioning of urban systems. One area of vulnerability is sensors, which collect data from the environment and transmit it to control systems for analysis and decision-making. These sensors are susceptible to cyber-attacks, which could result in the manipulation or spoofing of sensor data, leading to inaccurate insights and potentially harmful decisions (Jaïdi et al., 2016). Furthermore, compromised sensors could be exploited to gain unauthorized access to critical infrastructure or to launch attacks on other systems within the smart city ecosystem (Saber and Mazri, 2021). Control systems, which manage and regulate various processes and devices in smart cities, are also vulnerable to cyber threats. These systems often rely on interconnected networks and communication protocols,

making them susceptible to unauthorized access, manipulation, or disruption. Cyber-attacks targeting control systems could result in the disruption of essential services, such as transportation, utilities, or emergency response systems, posing significant risks to public safety and well-being (Shawe and McAndrew, 2023). Energy efficiency initiatives in smart cities, while beneficial for sustainability and cost savings, can also introduce cybersecurity vulnerabilities. Smart energy grids and systems rely on interconnected devices and networks to optimize energy usage and distribution. However, these systems are susceptible to cyber-attacks that could disrupt energy supply, cause power outages, or manipulate energy consumption data (Hemmati and Faraji, 2022). Ensuring the security and resilience of smart energy infrastructure is critical to maintaining reliable and efficient energy services in smart cities. Networks serve as the backbone of smart city infrastructure, facilitating communication and data exchange among diverse devices and systems. However, the interconnected nature of these networks also exposes them to cyber threats such as unauthorized access, data breaches, and denial of service. Safeguarding smart city networks necessitates robust encryption, access control, and monitoring mechanisms to efficiently detect and counter potential threats. Research into infrastructure vulnerabilities in smart cities has focused on developing innovative solutions to bolster cybersecurity and resilience. Mehdi et al. use machine learning algorithms to detect anomalies in sensor data, allowing early detection of cyber attacks or system failures (Houichi et al., 2021b). Additionally, Omotunde implemented secure communication protocols and encryption techniques to shield control systems and networks from unauthorized access and data tampering. Additionally, the study highlights the importance of integrating security considerations into the design and development of smart city infrastructure from the very beginning. This involves conducting thorough risk assessments, adhering to security-by-design principles, and adopting standards and best practices for securing critical infrastructure components. By addressing infrastructure threats and using research-based solutions, smart cities can increase cybersecurity and reduce the risk of emerging threats. To effectively combat an infrastructure crisis, a holistic approach focusing on vulnerability assessment, risk management planning, behavioral vulnerability and regular monitoring is essential. Routine assessments help identify vulnerabilities in physical infrastructures such as electrical grids, transportation networks, and telecommunications systems, allowing effective mitigation measures to be taken before they can be exploited by attackers.

Second, developing a robust risk management plan allows city officials to set priorities and effectively allocate resources to address identified vulnerabilities. Thirdly, employing ethical hacking practices enables security professionals to simulate cyberattacks and uncover potential security flaws, allowing for proactive remediation efforts. Finally, implementing continuous monitoring mechanisms ensures that any security incidents or anomalies are promptly detected and addressed, thereby enhancing the overall resilience of smart city infrastructure. By adopting these mitigation strategies, smart cities can strengthen their infrastructure resilience and mitigate the impact of potential cyber threats.

c. Network vulnerabilities: Network barriers pose serious threats to cybersecurity in smart cities, including many threats that can compromise the

integrity, confidentiality, and availability of information and services. Among these threats, Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks stand out. These attacks seek to inundate smart city networks and infrastructure with a deluge of malicious traffic, effectively rendering them inaccessible to legitimate users (Omotunde and Ahmed, 2023). These attacks can disrupt essential services, such as transportation systems, emergency response networks, or public utilities, leading to widespread inconvenience and potential safety hazards. Interception of communications represents another critical network vulnerability in smart cities, as it involves the unauthorized monitoring or eavesdropping on data transmissions between devices and systems (Tahirkheli et al., 2021). Cyber-attackers may exploit weaknesses in network protocols or encryption mechanisms to intercept sensitive information, such as personal data, financial transactions, or surveillance footage. This compromises the privacy and confidentiality of communications, potentially leading to identity theft, fraud, or surveillance abuses (Winn and Govern, 2009). Unauthorized access to smart city networks and systems poses a significant cybersecurity risk, as it allows malicious actors to gain unauthorized entry into critical infrastructure or sensitive data repositories. Attackers can exploit weaknesses in network security controls, such as weak passwords, unsupported software, or malicious hardware, to bypass authentication and gain privileged access (Apata et al., 2023). Once inside the network, attackers can escalate their privileges, steal data, or launch further cyber-attacks, causing widespread disruption and damage. Interoperability issues present another challenge in smart city networks, as they involve the seamless integration and communication between diverse systems and devices from different vendors or manufacturers (Kayode-Ajala, 2023). Incompatibilities or misconfigurations in network protocols or standards can create vulnerabilities that attackers may exploit to compromise the integrity or reliability of interconnected systems. Moreover, interoperability challenges can hinder the timely detection and response to cyber threats, exacerbating the risk of successful attacks (Rao and Subbarao, 2024). Research in the field of network vulnerabilities within smart cities has concentrated on devising advanced security measures and technologies to effectively mitigate these risks. Rao et al proposed new methods to detect and mitigate denial of service (DoS) and distributed denial of service (DDoS). This approach involves the use of machine learning-based anomaly detection algorithms and traffic filtering techniques (Abdulelah and Mustafa, 2020). Additionally, Abdulelah used advanced security protocols such as Transport Layer Security (TLS) to protect communication and data privacy (Ismagilova et al., 2022). Additionally, the study highlights the importance of implementing robust access control mechanisms and authentication protocols to prevent unauthorized access to smart city networks. This includes multi-factor authentication, role-based authentication (RBAC), and biometric authentication to authenticate users and devices accessing network resources. Additionally, there's an emphasis on the necessity for comprehensive vulnerability management programs and regular security audits to pinpoint and rectify potential security weaknesses in smart city networks effectively. To effectively address network vulnerabilities within smart city infrastructures, it's essential to implement comprehensive risk assessment methodologies and robust prevention systems. Regular risk assessments enable

organizations to identify and prioritize potential vulnerabilities within their network infrastructure. By analyzing the threat landscape and assessing the likelihood and impact of various cyber threats, organizations can proactively identify vulnerabilities and allocate resources accordingly to mitigate risks. Additionally, deploying advanced prevention systems, such as intrusion prevention systems (IPS) and firewalls, helps fortify network defenses and block malicious activities in real-time. These systems can detect and prevent unauthorized access attempts, malware infections, and other cyber threats and improve the overall effectiveness of smart city networks. By combining risk assessment practices with robust prevention systems, organizations can effectively mitigate network vulnerabilities and safeguard critical assets and data within smart city environments.

d. Data privacy leak: Data privacy represents a critical domain in cybersecurity risks within smart cities, encompassing various threats to the confidentiality, integrity, and control of sensitive data collected and processed within urban environments (Ribeiro-Navarrete et al., 2021). Data collection is a major challenge as smart city operations collect large amounts of data from sensors, control systems, and related devices. This information includes personal information about individuals and location information, which raises privacy concerns regarding acquisition, storage, and use (Lima et al., 2021). Unauthorized or excessive collection of data may violate individual rights and increase the risk of data breach or misuse. Data security is another key to data privacy in smart cities, focusing on protecting collected data from unauthorized access, disclosure, or tampering (Hasan et al., 2022). Weaknesses in data security measures, such as inadequate encryption, insecure storage practices, or vulnerabilities in data transmission protocols, can expose sensitive information to cyber threats (Shukla et al., 2022).

This presents substantial risks, such as identity theft, financial fraud, or unauthorized surveillance. Ensuring robust data security controls and encryption mechanisms is essential for mitigating these risks and safeguarding the confidentiality and integrity of data in smart city environments (Babikian, 2023). Data sharing and control present additional challenges in maintaining data privacy within smart cities, as they involve the dissemination and governance of collected data among various stakeholders, including government agencies, service providers, and third-party vendors. Poorly defined data sharing policies or insufficient access controls can lead to unauthorized data disclosures or breaches of privacy. Additionally, lack of transparency and user control over data sharing practices can erode public trust and confidence in smart city initiatives. Establishing guidelines and procedures for data sharing and giving individuals greater control over their data is important to adhere to privacy principles and respect user rights (Froomkin and Colangelo, 2020). Personal and location data pose specific privacy risks in smart city environments, as they provide insights into individuals' behaviors, movements, and preferences. Access to or misuse of personal information and location may result in inbound tracking, profiling or targeted advertising, compromising privacy and independence. Additionally, collecting and analyzing personal data from multiple sources raises concerns about data aggregation and re-identification, potentially leading to compromised privacy or discrimination (Rizi and Seno, 2022). Implementation of privacy-enhancing technologies, such as anonymization

techniques, multi-layered privacy, or data sharing methods, can help reduce these effects and protect people's privacy in smart city projects (Pratomo et al., 2023). Research on information privacy in smart cities tries to solve these problems with new solutions and methods to improve information and privacy. Pratomo et al. proposed effective detection and anonymization methods to obtain sensitive data and reduce the risk of unauthorized access or disclosure (Brauneck et al., 2023). In addition, Brauneck explored the use of privacy-enhancing technology as an integrated approach to enable data analysis and protection of individual privacy (Pasandi, 2024). Additionally, the study highlights the importance of following privacy principles and conducting privacy impact assessments (PIAs) to integrate privacy considerations into the development and deployment of smart city technology. This involves integrating privacy controls, such as granular consent mechanisms or purpose limitations, into data collection and processing workflows to ensure adherence to privacy regulations and standards. By leveraging research-driven methodologies and best practices, smart cities can bolster data privacy safeguards, mitigate privacy risks, and cultivate trust and confidence among residents regarding the responsible handling of their personal data (Zhou et al., 2018). Successfully addressing environmental privacy issues in a smart city requires a proactive approach to privacy using design principles. Implementing privacy by design means integrating privacy considerations into system design and operation from the beginning. By incorporating privacy and control-enhancing features into smart city infrastructure, organizations can reduce the risk of data breaches and compliance. Additionally, implementing mitigation measures helps limit the collection, storage and processing of personal and sensitive information to what is strictly necessary for the intended purpose. Open data practices, such as providing clear and easily accessible privacy policies and consent procedures, increase trust and enable people to make informed choices about their data. Further more, granting users control over their data through robust authentication and authorization mechanisms, along with providing rights such as access, rectification, and deletion of personal information, enhances transparency and accountability. Embracing these mitigation strategies enables organizations to uphold data privacy principles and safeguard the rights and interests of individuals within smart city ecosystems.

e. IoT devices issues: The proliferation of Internet of Things (IoT) devices poses a serious security problem in urban environments, as these connected devices often do not have strong security measures and these devices remain vulnerable to various cyber attacks (Sizov, 2024). One of the main concerns is the prevalence of inefficient authentication mechanisms for IoT devices, which provide opportunities for malicious actors to gain unauthorized access. Common problems include the use of passwords or simple passwords and lack of authentication; This makes IoT devices vulnerable to trust-based attacks such as brute force attacks or legitimate objects (Bhardwaj et al., 2024). Additionally, vulnerabilities inherent in IoT devices pose a considerable risk to smart city cybersecurity, as these devices may harbor software bugs, design flaws, or outdated firmware that attackers can exploit to compromise their security (Rafique et al., 2020). Such vulnerabilities may manifest in various forms, including remote code execution, privilege escalation, or denial-of-service (DoS) attacks, potentially allowing adversaries to seize control of IoT

devices or disrupt their normal functioning. The heterogeneous nature of IoT ecosystems further complicates vulnerability management, as different devices may have diverse software stacks and update mechanisms, making it challenging to ensure timely patching and mitigation of vulnerabilities (Lounis and Zulkernine, 2020). Insecure communication channels represent a critical security weakness in IoT devices deployed across smart city infrastructures. Many IoT devices transmit data over insecure protocols or unencrypted communication channels, exposing sensitive information to interception or tampering by eavesdroppers or malicious entities. Moreover, the absence of secure communication mechanisms exposes IoT devices to man-in-the-middle attacks, wherein adversaries can intercept and alter data exchanged between devices and backend systems, jeopardizing the confidentiality and integrity of transmitted data (Fan et al., 2023). Furthermore, supply chain attacks represent a substantial risk to the security of IoT devices in smart cities, given that these devices are frequently produced by third-party vendors and depend on intricate supply chains. Adversaries may target the supply chain to inject malicious hardware or software components into IoT devices during the manufacturing or distribution process, compromising their security and integrity. Such attacks can have far-reaching consequences, allowing attackers to establish persistent backdoors, steal sensitive data, or launch large-scale botnet attacks leveraging compromised IoT devices. Furthermore, the lack of security awareness among IoT device manufacturers, developers, and end-users exacerbates cybersecurity risks in smart city deployments (Xenofontos et al., 2021). Many IoT devices are designed with limited consideration for security best practices, prioritizing functionality and cost-effectiveness over security. Additionally, end-users may lack awareness of the security implications associated with IoT devices, leading to poor configuration practices or failure to apply security updates, leaving devices vulnerable to exploitation (Guerar et al., 2020). Research in the domain of IoT device security has focused on addressing these vulnerabilities and mitigating cybersecurity risks in smart city environments. Guerar have proposed enhanced authentication mechanisms to strengthen access control and prevent unauthorized access to IoT devices (Adel, 2023a). Moreover, research efforts have explored the use of secure boot mechanisms, runtime integrity verification, and containerization techniques to mitigate the impact of vulnerabilities and defend against supply chain attacks. Furthermore, Yuvaraj implemented a secure communication protocol based on Transport Layer Security (TLS) to encrypt data sent between IoT devices and backend systems, ensuring confidentiality and integrity. Additionally, researchers have advocated for the adoption of security-by-design principles and security-focused development frameworks to integrate security considerations into the entire lifecycle of IoT devices, from design and development to deployment and operation. By leveraging research-driven approaches and best practices, smart cities can enhance the security of IoT devices, mitigate cybersecurity risks, and ensure the integrity and resilience of their interconnected infrastructures. Additionally, many recent activities require robotic systems such as Unmanned Ground Vehicles (UGVs), terrestrial robots developed as an extension of human resources. These UGVs can have their basic motion mechanisms, such as acceleration, braking, and speed, controlled remotely, and with the integration of sensing and real-time

monitoring systems, they provide valuable tools for use in smart cities. This ideation model is further enhanced by using a web application for front and back-end management, creating a robust system for smart city applications (Vitunskaite et al., 2019). To address security challenges associated with IoT devices in smart city environments, implementing robust mitigation strategies is essential. Firstly, ensuring secure access controls and protocols is essential to prevent unauthorized access to IoT devices and sensitive data. By employing robust authentication mechanisms and limiting access to authorized users, organizations can reduce the likelihood of unauthorized manipulation or exploitation of IoT devices. Additionally, deploying secure communications protocols, such as Transport Layer Security (TLS) or Datagram Transport Layer Security (DTLS), encrypts data transmission between IoT devices and backend systems, guarding against interception and tampering. Moreover, implementing comprehensive security monitoring mechanisms enables organizations to identify and respond to suspicious activities or anomalies in real-time, enabling timely intervention to mitigate potential security breaches. By integrating these mitigation measures, organizations can bolster the security posture of IoT devices within smart city infrastructures, thereby minimizing risks and ensuring the integrity and confidentiality of transmitted and processed data by these devices.

f. Lack of security standards and regulation: Security standards play an important role in reducing cybersecurity risks in urban environments, but there are many problems that hinder their effectiveness (Atha et al., 2020). One significant challenge is the fragmented development of security standards and regulations, resulting in a lack of harmonization and consistency across different jurisdictions and sectors. This fragmentation leads to confusion among stakeholders and may create loopholes that adversaries can exploit to circumvent security measures. Moreover, the rapid evolution of technology often outpaces the development of relevant regulations, leaving smart city deployments vulnerable to emerging threats that existing standards fail to address adequately (Izario et al., 2020). The integration of legacy infrastructure poses another challenge to cybersecurity in smart cities, as outdated systems may lack built-in security features and compatibility with modern security standards. Legacy systems often rely on proprietary protocols or outdated encryption algorithms, making them susceptible to exploitation by adversaries (Benyahya et al., 2022). Additionally, the integration of legacy infrastructure with newer, more secure systems can introduce vulnerabilities and create potential points of entry for attackers to compromise the overall security posture of smart city deployments. Compliance complexity adds another layer of challenge to cybersecurity in smart cities, particularly concerning the diverse and overlapping regulatory requirements that govern data privacy, cybersecurity, and critical infrastructure protection (Scandizzo and Knudsen, 2024). Smart city stakeholders face the challenge of navigating a complex regulatory environment, which demands substantial resources and expertise to ensure compliance with relevant laws and regulations. Additionally, the lack of clear and consistent regulatory guidelines may result in compliance gaps or discrepancies, potentially exposing smart city initiatives to legal and regulatory uncertainties. Regulatory challenges are increasing cybersecurity concerns in smart cities, as regulators often struggle to keep up with

the rapid evolution of technology and emerging threats. Delays in updating regulations or adapting them to new technological developments can create regulatory gaps that adversaries can exploit to evade detection and prosecution. Moreover, regulatory uncertainty may deter investment in cybersecurity initiatives, as stakeholders may hesitate to commit resources to compliance efforts without clear guidance from regulators (Lyon, 2020). Lack of expertise presents a final challenge to effective cybersecurity regulation in smart cities, as many municipalities and organizations lack the necessary knowledge and skills to navigate complex regulatory requirements and implement robust security measures. The scarcity of cybersecurity experts worsens this issue, as organizations find it challenging to attract and retain skilled professionals capable of effectively addressing the constantly evolving cybersecurity landscape (Adel, 2023b). Additionally, the interdisciplinary nature of smart city cybersecurity requires collaboration among various stakeholders, including policymakers, regulators, industry experts, and cybersecurity professionals, further complicating efforts to develop and enforce effective security standards and regulations (Asaju, 2024). Research on security and regulation in smart cities has focused on addressing these issues and improving the effectiveness of cybersecurity management. Asaju proposed frameworks for harmonizing security standards and regulations across different jurisdictions, facilitating interoperability and consistency in compliance efforts [145]. Moreover, research efforts have explored the development of adaptive compliance frameworks capable of dynamically adjusting to evolving regulatory requirements and technological advancements, ensuring the resilience and agility of smart city deployments in the face of regulatory challenges. Furthermore, researchers have advocated for the development of cybersecurity capacity-building programs and educational initiatives to address the lack of expertise in smart city cybersecurity. By investing in training and professional development opportunities, municipalities and organizations can empower their personnel with the knowledge and skills needed to navigate regulatory complexities effectively and implement robust security measures (Telo, 2023b). Additionally, the research focuses on the importance of stakeholder collaboration and participation in regulatory processes so that regulatory frameworks reflect the diverse needs and perspectives of stakeholders in a smart city. By leveraging research-based approaches and best practices, smart cities can strengthen cybersecurity governance frameworks, increase regulatory compliance, and reduce cybersecurity risks. To effectively address security concerns and ensure robust cybersecurity frameworks in smart city environments, it is imperative to adopt comprehensive security standards and regulations. Firstly, the adoption of international standards provides a solid foundation for cybersecurity practices, aligning with globally recognized best practices and ensuring interoperability with international partners. Additionally, implementing smart grid security standards specifically tailored to the unique challenges of smart city infrastructures helps mitigate risks associated with energy distribution and management systems, safeguarding critical infrastructure against cyber threats. Moreover, articulating with local and national frameworks enables smart city initiatives to adhere to regulatory requirements and compliance mandates specific to their geographic regions. By aligning with local and national cybersecurity frameworks, organizations can ensure

consistency and adherence to legal and regulatory obligations, thereby enhancing the overall security posture of smart city ecosystems. These mitigation strategies facilitate the establishment of robust security standards and regulations tailored to the evolving threat landscape, ultimately contributing to the resilience and sustainability of smart city infrastructures.

g. Human misbehavior: Human behavior plays a critical role in cybersecurity risks within smart cities, with several common pitfalls posing significant challenges to the overall security posture (Kitchin, 2016). Misconfiguration stands out as a prominent risk factor, as human errors during the setup and configuration of smart city systems can inadvertently expose vulnerabilities and weaken defenses. Whether it's improperly configured network settings or mismanaged access controls, these misconfigurations can provide entry points for attackers to exploit and compromise smart city infrastructure. Weak passwords are another prevalent issue in smart city cybersecurity, as individuals often use easily guessable or reused passwords that are susceptible to brute-force attacks. Despite awareness campaigns and best practices advocating for strong, unique passwords, many users still prioritize convenience over security, putting smart city systems at risk of unauthorized access and data breaches (Abdel-Rahman, 2023). Moreover, the widespread adoption of default passwords and the lack of password hygiene exacerbate this risk, underscoring the need for robust password policies and user education initiatives. Software updates are essential for maintaining the security of smart city infrastructure, yet human behavior often presents barriers to timely patching and updates. Whether due to complacency, ignorance, or logistical challenges, many individuals and organizations delay or ignore software updates, leaving systems vulnerable to known exploits and vulnerabilities (Bailey and Nyabola, 2021). This reluctance to update software can have severe consequences in smart cities, where interconnected systems and devices rely on up-to-date software to defend against evolving cyber threats. Dependency on technology is another factor that influences human behavior and cybersecurity risks in smart cities. As cities become increasingly reliant on technology to deliver essential services and streamline operations, the consequences of technology failures or cyber-attacks become more pronounced (Chaudhary, 2024). However, this reliance on technology can also lead to complacency and overconfidence in the resilience of smart city systems, potentially overlooking critical security gaps and vulnerabilities. Digital exclusion presents a unique challenge to smart city cybersecurity, as marginalized communities and individuals lacking access to digital resources may be disproportionately impacted by cyber threats. The digital divide exacerbates inequalities in cybersecurity resilience, leaving vulnerable populations at greater risk of exploitation and harm. Moreover, digital exclusion can hinder efforts to implement inclusive cybersecurity education and awareness initiatives, further widening the gap between cybersecurity haves and have-nots. Research on human behavior and cybersecurity in smart cities attempts to solve these problems through technological solutions and ethical practices. Additionally, Chaudhary explored the use of nudges and incentives to promote desirable cybersecurity behaviors, such as timely software updates and adherence to security best practices. Furthermore, researchers have advocated for the integration of cybersecurity education and awareness initiatives into smart city planning and development efforts, ensuring that

residents, businesses, and policymakers are equipped with the knowledge and skills needed to mitigate cybersecurity risks effectively. By fostering a culture of cybersecurity awareness and resilience, smart cities can empower individuals to make informed decisions and take proactive steps to protect themselves and their communities from cyber threats. Addressing cybersecurity risks stemming from human behavior requires a multifaceted approach that combines education, awareness, and ethical guidelines. First, investing in education and awareness programs helps equip people with the knowledge and skills needed to effectively detect and mitigate threats. Additionally, establishing ethical guidelines and promoting ethical behavior among stakeholders fosters a culture of responsible digital citizenship and accountability. Leveraging behavioral analytics and predictive models enables organizations to identify and address potential security incidents proactively, leveraging insights into user behavior to enhance threat detection and response capabilities. Moreover, fostering collaboration and partnerships among stakeholders encourages information sharing and collective action in combating cyber threats. Lastly, engaging with the community promotes a sense of ownership and responsibility for cybersecurity, fostering a collaborative environment where individuals and organizations work together to safeguard smart city infrastructures. By implementing these mitigation strategies, smart city initiatives can effectively address cybersecurity risks associated with human behavior, creating a safer and more resilient urban environment for all stakeholders.

4.2. NIST-based analysis

Diverse standards, models and frameworks are defined in literature for incorporating trust-risk awareness solutions in smart cities infrastructures like the NIST, ISO, FAIR frameworks (Shahzad et al., 2021). Risk Management (RM) based approaches are key solutions for handling smart cities cyber security issues. RM techniques consist mainly in the identification of cyber threats, the assessment of their associated risks and the implementation of mitigation strategies. Within smart city environments, it is highly recommended to consider adaptive and dynamic RM approaches (Ksibi et al., 2023). taking benefits from AI techniques while preserving the compliance with standards. In analyzing the cybersecurity threats in smart cities, applying the NIST Risk Management Framework (NIST RMF) offers a structured and methodical approach to managing and mitigating risks. The NIST RMF guides smart cities through a lifecycle of risk management that includes preparation, categorization, control selection, implementation, assessment, authorization, and continuous monitoring. This approach not only enhances the security posture of smart cities but also ensures alignment with industry standards and regulatory requirements.

Preparation involves a comprehensive understanding of the smart city ecosystem, identifying all critical assets and the relationships between interconnected systems. For smart cities, this means mapping out components such as IoT devices, data networks, and physical infrastructure. During this phase, it is essential to anticipate potential threats, assess existing vulnerabilities, and prepare for effective risk management strategies tailored to the city's unique context.

Categorization under the NIST RMF requires identifying the impact levels of various systems and data within the smart city. This step helps prioritize security efforts. For example, a breach in a smart grid system would be classified as high impact due to its potential to disrupt essential services, whereas a breach in a public information system might be lower in priority. By categorizing systems based on their criticality, resources can be allocated efficiently, ensuring that the most significant risks are addressed first.

Control selection is crucial in mitigating identified risks. In the context of smart cities, selecting appropriate controls from the NIST SP 800-53 catalog allows for targeted interventions. For example, employing strong access control measures, such as multi-factor authentication, is vital to prevent unauthorized access to critical infrastructure. Simultaneously, ensuring robust encryption protocols for data in transit and at rest is essential to protect sensitive information. These controls should be chosen with a focus on both preventive and detective measures, ensuring a layered defense strategy.

Implementation of these controls must be integrated seamlessly into the existing smart city infrastructure. This step goes beyond merely deploying technical solutions—it involves ensuring that all stakeholders, from city administrators to end-users, are aligned with the security objectives. For instance, regular updates and patch management processes must be enforced across all IoT devices to minimize vulnerabilities. Additionally, building security into the system design from the outset, rather than as an afterthought, can significantly reduce potential risks.

Assessment within the NIST RMF is about verifying the effectiveness of the implemented controls. In smart cities, this requires continuous vulnerability assessments, penetration testing, and audits. For example, regularly testing the resilience of critical infrastructure against simulated cyber-attacks can reveal weaknesses that need addressing. This step is also an opportunity to refine and enhance controls, ensuring they adapt to evolving threats.

Authorization involves a formal risk acceptance process, where smart city systems are given the green light to operate based on their assessed risk levels. In this context, city authorities must carefully evaluate whether the remaining risks are within acceptable thresholds. This ensures that only systems that meet stringent security requirements are allowed to operate, reducing the likelihood of catastrophic failures.

Monitoring is an ongoing process, critical to the dynamic nature of cybersecurity in smart cities. Continuous monitoring of networks, IoT devices, and user activities allows for real-time detection of anomalies or malicious behavior. Automated tools that provide alerts and enable swift responses to incidents are essential in maintaining the security and resilience of smart city systems. Moreover, continuous monitoring ensures that as the threat landscape evolves, smart cities can adapt their security measures accordingly.

Through the application of the NIST RMF, smart cities can create a robust cybersecurity framework that not only addresses immediate threats but also evolves with the changing technological landscape. This ensures that smart cities remain resilient and capable of protecting their critical infrastructures and citizens against cyber threats.

4.3. Recommendations

The opportunities for change are huge in the context of smart cities, where technology and urban development merge. As we face the challenges of integrating technology into urban environments, it is important to prioritize cybersecurity to protect against emerging threats. To take full advantage of the smart city while reducing cyber risks, the following recommendations are important:

Integrating Smart and Cyber City Strategies: Cities should develop comprehensive security strategies that are compatible with the overall smart vision. This involves conducting in-depth assessments to identify, evaluate and mitigate risks associated with urban technology integration. By integrating cybersecurity considerations into all aspects of smart city planning, cities can meet the challenge of securing and verifying their digital infrastructure.

Cyber and data governance transformation: Establishing a strong governance framework to manage information, assets and infrastructure is essential. Cities need to define roles and responsibilities in the smart environment and promote multi-institutional collaboration to effectively address technology challenges. Additionally, effective partnerships with businesses, academia and industry can increase cyber capacity, address knowledge gaps and increase cyber resilience.

Developing effective partnerships to improve cyber skills: With the ongoing cyber skills gap, cities must use new methods to improve the cyber skills of their citizens. Effective partnerships with service providers and new recruitment initiatives can help cities increase their cyber capabilities and counter growing threats. By using a collaborative approach to cybersecurity management, cities can leverage the collective expertise of government, academia, and the private sector to better protect themselves and respond effectively to cyber incidents.

As a result, the journey to realize the full potential of smart cities depends on effectively managing cyber risks and creating a strong ecosystem. By prioritizing cybersecurity, integrating smart city and cyber strategies, creating governance frameworks, and developing effective partnerships, cities can meet the challenges of the digital age and pave the way for a better urban future. As technology continues to evolve, research and collaboration will be important to overcome these challenges and ensure the long-term development of smart city initiatives.

5. Conclusion

In this study, we have explored cybersecurity challenges that smart cities face, emphasizing the vulnerabilities inherent in the interconnected systems that define these urban environments. While the integration of technologies such as IoT, AI, and data analytics offers immense potential for enhancing urban life, it also introduces significant risks, particularly in areas like access control, data privacy, network security, and IoT device management. Our analysis underscored the need for comprehensive cybersecurity frameworks that not only address current threats but are also adaptable to future challenges. Looking ahead, future work should focus on developing adaptive security systems that can dynamically respond to new and emerging threats, leveraging AI and machine learning to anticipate and neutralize attacks in real-time. Additionally, the exploration of advanced privacy-preserving

technologies, such as homomorphic encryption and differential privacy, is essential for protecting sensitive data while enabling the data-driven insights crucial for smart city operations. The development of global interoperability standards will be vital to ensure secure and efficient communication across diverse systems within smart cities. Addressing human factors in cybersecurity remains critical, with a focus on creating user-friendly security solutions that promote cybersecurity awareness among citizens and reduce the risk of human error. Furthermore, as smart cities continue to evolve, the need for robust regulatory frameworks that can keep pace with technological advancements becomes increasingly important. Future research must explore how governments can develop and enforce regulations that balance innovation with security. By addressing these areas, ongoing collaboration between policymakers, industry stakeholders, and academia will be crucial in ensuring that smart cities are secure, resilient, and capable of meeting the needs of their citizens.

Author contributions: Conceptualization, MH and FJ; methodology, MH; software, MH; validation, MH, FJ and AB; formal analysis, MH; investigation, MH; resources, MH; data curation, MH; writing—original draft preparation, MH; writing—review and editing, MH; visualization, MH; supervision, FJ and AB; project administration, MH; funding acquisition, FJ. All authors have read and agreed to the published version of the manuscript.

Conflict of interest: The authors declare no conflict of interest.

References

Abdel-Rahman, M. (2023). Advanced cybersecurity measures in IT service operations and their crucial role in safeguarding enterprise data in a connected world. Eigenpub Review of Science and Technology, 7(1), 138-158.

Abdulelah, A. J., & Mustafa, A. S. (2020). Advanced Secure Architecture for The Internet of Things based on DTLS Protocol. 2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), 1–5. https://doi.org/10.1109/ismsit50672.2020.9254700

Access 17.0M+ vector icons & stickers. (2024). Download Free Icons and Stickers for your projects. Available online: https://www.flaticon.com (accessed on 3 May 2024).

Adel, A. (2023). Unlocking the Future: Fostering Human–Machine Collaboration and Driving Intelligent Automation through Industry 5.0 in Smart Cities. Smart Cities, 6(5), 2742–2782. https://doi.org/10.3390/smartcities6050124

Ahmad, R., Wazirali, R., & Abu-Ain, T. (2022). Machine Learning for Wireless Sensor Networks Security: An Overview of Challenges and Issues. Sensors, 22(13), 4730. https://doi.org/10.3390/s22134730

Ahmed, S., & Khan, M. (2023). Securing the Internet of Things (IoT): A comprehensive study on the intersection of cybersecurity, privacy, and connectivity in the IoT ecosystem. AI, IoT and the Fourth Industrial Revolution Review, 13(9), 1-17.

AlQahtani, A. A. S., Alshayeb, T., Nabil, M., et al. (2024). Leveraging Machine Learning for Wi-Fi-Based Environmental Continuous Two-Factor Authentication. IEEE Access, 12, 13277–13289. https://doi.org/10.1109/access.2024.3356351

Amin, S. U., & Hossain, M. S. (2021). Edge Intelligence and Internet of Things in Healthcare: A Survey. IEEE Access, 9, 45–59. https://doi.org/10.1109/access.2020.3045115

Angelidou, M., Psaltoglou, A., Komninos, N., et al. (2017). Enhancing sustainable urban development through smart city applications. Journal of Science and Technology Policy Management, 9(2), 146–169. https://doi.org/10.1108/jstpm-05-2017-0016

Apata, O., Bokoro, P. N., & Sharma, G. (2023). The Risks and Challenges of Electric Vehicle Integration into Smart Cities. Energies, 16(14), 5274. https://doi.org/10.3390/en16145274

Asaju, B. J. (2024). Standardization and regulation of V2X cybersecurity: analyzing the current landscape, identifying gaps, and proposing frameworks for harmonization. Advances in Deep Learning Techniques, 4(1), 33-52.

Azeez, O. H., Sarah, K. E., Adekunle, A. A., et al. (2024). Cybersecurity In Banking: A Global Perspective with A Focus on Nigerian Practices. Computer Science & IT Research Journal, 5(1), 41–59. https://doi.org/10.51594/csitrj.v5i1.701

Azzedin, F. (2023). Mitigating Denial of Service Attacks in RPL-Based IoT Environments: Trust-Based Approach. IEEE Access, 11, 129077–129089. https://doi.org/10.1109/access.2023.3331030

Babikian, J. (2023). Navigating Legal Frontiers: Exploring Emerging Issues in Cyber Law. Revista Espanola de Documentacion Cientifica, 17(2), 95-109.

Bailey, L. E., & Nyabola, N. (2021). Digital Equity as an Enabling Platform for Equality and Inclusion. Available online: https://cic. nyu. edu/resources/digital-equity-as-an-enabling-platform-for-equality-and-inclusion (accessed on 12 May 2024).

Bakshi, G., & Sahu, H. (2022). WSN Security. Computational Intelligence for Wireless Sensor Networks, 151–174. https://doi.org/10.1201/9781003102397-9

Barbera, S. L. (2023). Revolutionizing Italian Homes: Embracing the Smart Home Era in the Housing Landscape. Research square. https://doi.org/10.21203/rs.3.rs-3272478/v1

Belavagi, M. C., & Muniyal, B. (2022). Improved Intrusion Detection System using Quantal Response Equilibrium-based Game Model and Rule-based Classification. International Journal of Communication Networks and Information Security (IJCNIS), 13(1). https://doi.org/10.17762/ijcnis.v13i1.4875

Benyahya, M., Collen, A., Kechagia, S., et al. (2022). Automated city shuttles: Mapping the key challenges in cybersecurity, privacy and standards to future developments. Computers & Security, 122, 102904. https://doi.org/10.1016/j.cose.2022.102904

Bhardwaj, A., Bharany, S., Abulfaraj, A. W., et al. (2024). Fortifying home IoT security: A framework for comprehensive examination of vulnerabilities and intrusion detection strategies for smart cities. Egyptian Informatics Journal, 25, 100443. https://doi.org/10.1016/j.eij.2024.100443

Bibri, S. E., Alexandre, A., Sharifi, A., et al. (2023). Environmentally sustainable smart cities and their converging AI, IoT, and big data technologies and solutions: an integrated approach to an extensive literature review. Energy Informatics, 6(1). https://doi.org/10.1186/s42162-023-00259-2

Böhm, F., Dietz, M., Preindl, T., et al. (2021). Augmented Reality and the Digital Twin: State-of-the-Art and Perspectives for Cybersecurity. Journal of Cybersecurity and Privacy, 1(3), 519–538. https://doi.org/10.3390/jcp1030026

Boukerche, A., & Coutinho, R. W. L. (2019). Crowd Management: The Overlooked Component of Smart Transportation Systems. IEEE Communications Magazine, 57(4), 48–53. https://doi.org/10.1109/mcom.2019.1800641

Bouramdane, A. A. (2023). Optimal Water Management Strategies: Paving the Way for Sustainability in Smart Cities. Smart Cities, 6(5), 2849–2882. https://doi.org/10.3390/smartcities6050128

Brauneck, A., Schmalhorst, L., Kazemi Majdabadi, M. M., et al. (2023). Federated Machine Learning, Privacy-Enhancing Technologies, and Data Protection Laws in Medical Research: Scoping Review. Journal of Medical Internet Research, 25, e41588. https://doi.org/10.2196/41588

Chandramouli, D., Liebhart, R., & Pirskanen, J. (2019). 5G for the Connected World. Wiley Online Library. https://doi.org/10.1002/9781119247111

Chaudhary, S. (2024). Driving behavior change with cybersecurity awareness. Computers & Security, 142, 103858. https://doi.org/10.1016/j.cose.2024.103858

Dağtaş, S., Pekhteryev, G., Şahinoğlu, Z., et al. (2008). Real-Time and Secure Wireless Health Monitoring. International Journal of Telemedicine and Applications, 2008, 1–10. https://doi.org/10.1155/2008/135808

Data Science and Security. (2022). Lecture Notes in Networks and Systems. Springer Nature Singapore.

De Nicola, A., & Villani, M. L. (2021). Smart City Ontologies and Their Applications: A Systematic Literature Review. Sustainability, 13(10), 5578. https://doi.org/10.3390/su13105578

Decision Making and Security Risk Management for IoT Environments. (2024). Advances in Information Security. Springer International Publishing.

Demertzi, V., Demertzis, S., & Demertzis, K. (2023). An Overview of Cyber Threats, Attacks and Countermeasures on the Primary Domains of Smart Cities. Applied Sciences, 13(2), 790. https://doi.org/10.3390/app13020790

Dou, X., Chen, W., Zhu, L., et al. (2023). Machine Learning for Smart Cities: A Comprehensive Review of Applications and Opportunities. International Journal of Advanced Computer Science and Applications, 14(9). https://doi.org/10.14569/ijacsa.2023.01409104

Duggineni, S. (2023). Data Integrity and Risk. Open Journal of Optimization, 12(02), 25–33. https://doi.org/10.4236/ojop.2023.122003

Egbert, S., & Leese, M. (2020). Criminal Futures: Predictive Policing and Everyday Police Work. CrimRxiv. https://doi.org/10.21428/cb6ab371.17e3e7ab

Fan, J., Yang, W., Liu, Z., et al. (2023). Understanding Security in Smart City Domains From the ANT-Centric Perspective. IEEE Internet of Things Journal, 10(13), 11199–11223. https://doi.org/10.1109/jiot.2023.3252040

Froomkin, M., & Colangelo, Z. (2020). Privacy as Safety. Wash. L. Rev., 95, 141.

Ghorbel, A., Ghorbel, M., & Jmaiel, M. (2021). Accountable privacy preserving attribute-based access control for cloud services enforced using blockchain. International Journal of Information Security, 21(3), 489–508. https://doi.org/10.1007/s10207-021-00565-4

Gracias, J. S., Parnell, G. S., Specking, E., et al. (2023). Smart Cities—A Structured Literature Review. Smart Cities, 6(4), 1719–1743. https://doi.org/10.3390/smartcities6040080

Guerar, M., Verderame, L., Merlo, A., et al. (2020). CirclePIN. ACM Transactions on Cyber-Physical Systems, 4(3), 1–19. https://doi.org/10.1145/3365995

Hasan, M. K., Ghazal, T. M., Saeed, R. A., et al. (2021). A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things. IET Communications, 16(5), 421–432. Portico. https://doi.org/10.1049/cmu2.12301

Hemmati, R., & Faraji, H. (2022). Identification of cyber-attack/outage/fault in zero-energy building with load and energy management strategies. Journal of Energy Storage, 50, 104290. https://doi.org/10.1016/j.est.2022.104290

Hoang, T. V. (2024). Impact of Integrated Artificial Intelligence and Internet of Things Technologies on Smart City Transformation. Journal of Technical Education Science, 19(1), 64–73. https://doi.org/10.54644/jte.2024.1532

Houichi, M., Jaidi, F., & Bouhoula, A. (2022). Analysis of Smart Cities Security: Challenges and Advancements. In: Proceedings of 2022 15th International Conference on Security of Information and Networks (SIN); 11-13 November 2022; Sousse, Tunisia.

Houichi, M., Jaidi, F., & Bouhoula, A. (2023). A Comprehensive Study of Intrusion Detection within Internet of Things-based Smart Cities: Synthesis, Analysis and a Novel Approach. 2023 International Wireless Communications and Mobile Computing (IWCMC), 8, 505–511. https://doi.org/10.1109/iwcmc58020.2023.10182948

Islam, A. I. A., Anthony, C. A., Shedrack, O., et al. (2024). Cybersecurity Challenges in Smart Cities: A Case Review of African Metropolises. Computer Science & IT Research Journal, 5(2), 254–269. https://doi.org/10.51594/csitrj.v5i2.756

Ismagilova, E., Hughes, L., Rana, N. P., et al. (2020). Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework. Information Systems Frontiers, 24(2), 393–414. https://doi.org/10.1007/s10796-020-10044-1

Jaïdi, F., Labbene Ayachi, F., & Bouhoula, A. (2018). A Methodology and Toolkit for Deploying Reliable Security Policies in Critical Infrastructures. Security and Communication Networks, 2018, 1–22. https://doi.org/10.1155/2018/7142170

Jaïdi, F., Labbene-Ayachi, F., & Bouhoula, A. (2016). Advanced Techniques for Deploying Reliable and Efficient Access Control: Application to E-healthcare. Journal of Medical Systems, 40(12). https://doi.org/10.1007/s10916-016-0630-2

James, E., & Rabbi, F. (2023). Fortifying the IoT Landscape: Strategies to Counter Security Risks in Connected Systems. Tensorgate Journal of Sustainable Technology and Infrastructure for Developing Countries, 6(1), 32-46.

Jeong, H., Shen, Y., Jeong, J., & Oh, T. (2021). A comprehensive survey on vehicular networking for safe and efficient driving in smart transportation: A focus on systems, protocols, and applications. Vehicular Communications, 31, 100349. https://doi.org/10.1016/j.vehcom.2021.100349

Jha, A., & Jha, A. (2024). Securing tomorrow's urban frontiers: A holistic approach to cybersecurity in smart cities. Information System and Smart City, 3(1). https://doi.org/10.59400/issc.v3i1.418

Jia, M., Komeily, A., Wang, Y., et al. (2019). Adopting Internet of Things for the development of smart buildings: A review of enabling technologies and applications. Automation in Construction, 101, 111–126. https://doi.org/10.1016/j.autcon.2019.01.023

Ji-Young, K., Jong In, L., & Kyoung Gon, K. (2019). The All-Purpose Sword: North Korea's Cyber Operations and Strategies. 2019 11th International Conference on Cyber Conflict (CyCon), 5, 1–20. https://doi.org/10.23919/cycon.2019.8756954

Judijanto, L., Putra, H. N., Zani, B. N., et al. (2024). E-Health and Digital Transformation in Increasing Accessibility of Health Services. Journal of World Future Medicine, Health and Nursing, 2(1), 119–132. https://doi.org/10.70177/health.v2i1.720

Kalunga, J., Tembo, S., & Phiri, J. (2020). Development of Access Control Mechanism Based on Fingerprint Biometrics and Mobile Phone Identityfor Industrial Internet of ThingsCritical Infrastructure Protection. International Journal of Advances in Scientific Research and Engineering, 6(12), 15–34. https://doi.org/10.31695/ijasre.2020.33940

Kanellopoulos, D., Sharma, V. K., Panagiotakopoulos, T., et al. (2023). Networking Architectures and Protocols for IoT Applications in Smart Cities: Recent Developments and Perspectives. Electronics, 12(11), 2490. https://doi.org/10.3390/electronics12112490

Karale, A. (2021). The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws. Internet of Things, 15, 100420. https://doi.org/10.1016/j.iot.2021.100420

Kavitha, J., Rao, P. S. V. S., & Babu, G. C. (2023). Energy Efficient Resource Utilization of Cloud Computing Environments for Deployment Models. 2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS), 26, 1111–1119. https://doi.org/10.1109/icaiss58487.2023.10250648

Kayode-Ajala, O. (2023). Applications of Cyber Threat Intelligence (CTI) in financial institutions and challenges in its adoption. Applied Research in Artificial Intelligence and Cloud Computing, 6(8), 1-21.

Khan, M. Y. (2023). Cyber Security: Recent Cyber-Attacks as A Challenge to National Economic Security. International Journal of Modern Sciences and Multidisciplinary Studies (Ijmsms), 2(01), 72-100.

Kim, K., Alshenaifi, I. M., Ramachandran, S., et al. (2023). Cybersecurity and Cyber Forensics for Smart Cities: A Comprehensive Literature Review and Survey. Sensors, 23(7), 3681. https://doi.org/10.3390/s23073681

Kim, K., Cho, K., Lim, J., et al. (2020). What's your protocol: Vulnerabilities and security threats related to Z-Wave protocol. Pervasive and Mobile Computing, 66, 101211. https://doi.org/10.1016/j.pmcj.2020.101211

Kim, K., Kim, J. S., Jeong, S., et al. (2021). Cybersecurity for autonomous vehicles: Review of attacks and defense. Computers & Security, 103, 102150. https://doi.org/10.1016/j.cose.2020.102150

Kitchin, R. (2016). Getting smarter about smart cities: Improving data privacy and data security. Sensors. https://doi.org/10.3390/s22239338

Krishna, S. R., Rathor, K., Ranga, J., et al. (2023). Artificial Intelligence Integrated with Big Data Analytics for Enhanced Marketing. In 2023 International Conference on Inventive Computation Technologies (ICICT). IEEE; pp. 1073-1077.

Ksibi, S., Jaidi, F., & Bouhoula, A. (2023). IoMT Security Model based on Machine Learning and Risk Assessment Techniques. 2023 International Wireless Communications and Mobile Computing (IWCMC), 11, 614–619. https://doi.org/10.1109/iwcmc58020.2023.10182654

Lansky, J., Sadrishojaei, M., Rahmani, A. M., et al. (2022). Development of a Lightweight Centralized Authentication Mechanism for the Internet of Things Driven by Fog. Mathematics, 10(22), 4166. https://doi.org/10.3390/math10224166

Li, H., Wang, X., Feng, Y., et al. (2024). Integration Methods and Advantages of Machine Learning with Cloud Data Warehouses. International Journal of Computer Science and Information Technology, 2(1), 348–358. https://doi.org/10.62051/ijcsit.v2n1.36

Liu, Y., Yu, F. R., Li, X., et al. (2020). Blockchain and Machine Learning for Communications and Networking Systems. IEEE Communications Surveys & Tutorials, 22(2), 1392–1431. https://doi.org/10.1109/comst.2020.2975911

Löfgren, K., & Webster, C. W. R. (2020). The value of Big Data in government: The case of smart cities. Big Data & Society, 7(1), 205395172091277. https://doi.org/10.1177/2053951720912775

Lounis, K., & Zulkernine, M. (2020). Attacks and Defenses in Short-Range Wireless Technologies for IoT. IEEE Access, 8, 88892–88932. https://doi.org/10.1109/access.2020.2993553

Lyon, V. (2020). Exploring Strategies for Recruiting and Retaining Diverse Cybersecurity Professionals [PhD thesis]. Walden University.

Ma, C. (2021). Smart city and cyber-security; technologies used, leading challenges and future recommendations. Energy Reports, 7, 7999–8012. https://doi.org/10.1016/j.egyr.2021.08.124

Majdoubi, D. E., Bakkali, H., & Sadki, S. (2020). Towards Smart Blockchain-Based System for Privacy and Security in a Smart City environment. In: Proceedings of 2020 5th International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications (CloudTech); 24–26 November 2020; Marrakesh, Morocco.

Marín Díaz, G., Galdón Salvador, J. L., & Galán Hernández, J. J. (2023). Smart Cities and Citizen Adoption: Exploring Tourist Digital Maturity for Personalizing Recommendations. Electronics, 12(16), 3395. https://doi.org/10.3390/electronics12163395

Markovic, D. S., Zivkovic, D., Branovic, I., et al. (2013). Smart power grid and cloud computing. Renewable and Sustainable Energy Reviews, 24, 566–577. https://doi.org/10.1016/j.rser.2013.03.068

Meng, X., & Zhu, L. (2024). Augmenting cybersecurity in smart urban energy systems through IoT and blockchain technology within the Digital Twin framework. Sustainable Cities and Society, 106, 105336. https://doi.org/10.1016/j.scs.2024.105336

Miller, C., & Valasek, C. (2015). Remote exploitation of an unaltered passenger vehicle. Black Hat USA, 2015(S 91), 1-91.

Miranda, R., Alves, C., Sousa, R., et al. (2024). Revolutionising the Quality of Life: The Role of Real-Time Sensing in Smart Cities. Electronics, 13(3), 550. https://doi.org/10.3390/electronics13030550

Mortaheb, R., & Jankowski, P. (2023). Smart city re-imagined: City planning and GeoAI in the age of big data. Journal of Urban Management, 12(1), 4–15. https://doi.org/10.1016/j.jum.2022.08.001

Mun, M., Reddy, S., Shilton, K., et al. (2009). PEIR, the personal environmental impact report, as a platform for participatory sensing systems research. In: Proceedings of the 7th International Conference on Mobile Systems, Applications, and Services; 22 June 2009.

Nastjuk, I., Trang, S., & Papageorgiou, E. I. (2022). Smart cities and smart governance models for future cities. Electronic Markets, 32(4), 1917–1924. https://doi.org/10.1007/s12525-022-00609-0

Nguyen, L., Phan, B., Zhang, L., et al. (2024). An Efficient Approach for Securing Audio Data in AI Training with Fully Homomorphic Encryption. Available online: https://doi.org/10.36227/techrxiv.170956397.78402834/v1 (accessed on 12 May 2024).

Nurthen II, J. M. (2023). Cybersecurity Risk Assessment Matrix (CRAM): A System-Theoretic Approach to Balancing Operational and Cybersecurity Risk in the Management of Transient Cyber Assets (TCA) in the Maintenance of Operational Technology (OT) [PhD thesis]. Massachusetts Institute of Technology.

Omotunde, H., & Ahmed, M. (2023). A Comprehensive Review of Security Measures in Database Systems: Assessing Authentication, Access Control, and Beyond. Mesopotamian Journal of Cyber Security, 115–133. https://doi.org/10.58496/mjcsc/2023/016

Panahi Rizi, M. H., & Hosseini Seno, S. A. (2022). A systematic review of technologies and solutions to improve security and privacy protection of citizens in the smart city. Internet of Things, 20, 100584. https://doi.org/10.1016/j.iot.2022.100584

Panda, P. K., & Chattopadhyay, S. (2020). A secure mutual authentication protocol for IoT environment. Journal of Reliable Intelligent Environments, 6(2), 79–94. https://doi.org/10.1007/s40860-020-00098-y

Pasandi, F. B. (2024). Creative Organic Smart Spaces and Communities: Leveraging Technology to Fight Socio-Environmental Impacts. Available online: https://hal.science/hal-04527432 (accessed on 17 May 2024).

Petrova, M., & Tairov, I. (2022). Solutions to Manage Smart Cities' Risks in Times of Pandemic Crisis. Risks, 10(12), 240. https://doi.org/10.3390/risks10120240

Pratomo, A. B., Mokodenseho, S., & Aziz, A. M. (2023). Data Encryption and Anonymization Techniques for Enhanced Information System Security and Privacy. West Science Information System and Technology, 1(01), 1–9. https://doi.org/10.58812/wsist.v1i01.176

Principles and Applications of Narrowband Internet of Things (NBIoT). (2021). Advances in Wireless Technologies and Telecommunication. IGI Global. https://doi.org/10.4018/978-1-7998-4775-5

Proceedings of the 6th Brazilian Technology Symposium (BTSym'20). (2021). Smart Innovation, Systems and Technologies. Springer International Publishing.

Proceedings of the 7th Brazilian Technology Symposium (BTSym'21). (2022). Smart Innovation, Systems and Technologies. Springer International Publishing.

Rafique, W., Qi, L., Yaqoob, I., et al. (2020). Complementing IoT Services Through Software Defined Networking and Edge Computing: A Comprehensive Survey. IEEE Communications Surveys & Tutorials, 22(3), 1761–1804. https://doi.org/10.1109/comst.2020.2997475

Rahman, K., Khan, M. A., Afghah, F., et al. (2024). An Efficient Authentication and Access Control Protocol for Securing UAV Networks Against Anomaly-Based Intrusion. IEEE Access, 12, 62750–62764. https://doi.org/10.1109/access.2024.3395494

Raj, P., Akilandeswari, J., & Marimuthu, M. (2022). The edge AI paradigm: Technologies, platforms and use cases. Edge/Fog Computing Paradigm: The Concept Platforms and Applications, 139–182. https://doi.org/10.1016/bs.adcom.2022.02.003

Rajendran, S., Sabharwal, M., Ghinea, G., et al. (2022). IoT and Big Data Analytics for Smart Cities. Chapman and Hall/CRC. https://doi.org/10.1201/9781003217404

Rao, G. S., & Subbarao, P. K. (2024). A Novel Framework for Detection of DoS/DDoS Attack Using Deep Learning Techniques, and An Approach to Mitigate the Impact of DoS/DDoS attack in Network Environment. International Journal of Intelligent Systems and Applications in Engineering, 12(1), 450-466.

Rehan, H. (2023). Internet of Things (IoT) in Smart Cities: Enhancing Urban Living Through Technology. Journal of Engineering and Technology, 5(1), 1-16.

Rejeb, A., Rejeb, K., Simske, S. J., et al. (2021). Blockchain technology in the smart city: a bibliometric review. Quality & Quantity, 56(5), 2875–2906. https://doi.org/10.1007/s11135-021-01251-2

Remotti, L. A. (2021). IoT innovation clusters in Europe and the case for public policy. Data & Policy, 3. https://doi.org/10.1017/dap.2021.16

Rhoda, A. A., Kehinde, F, A., Ndubuisi, L. N., et al. (2024). Reviewing big data's role in the digital economy: USA and Africa focus. World Journal of Advanced Research and Reviews, 21(2), 085–095. https://doi.org/10.30574/wjarr.2024.21.2.0396

Ribeiro-Navarrete, S., Saura, J. R., & Palacios-Marqués, D. (2021). Towards a new era of mass data collection: Assessing pandemic surveillance technologies to preserve user privacy. Technological Forecasting and Social Change, 167, 120681. https://doi.org/10.1016/j.techfore.2021.120681

Sabbar Zamel, L., & Rokan Naif, J. (2023). An Overview Smart Assistant System for Old People Using Internet of Things. Iraqi Journal for Computers and Informatics, 49(2), 28–36. https://doi.org/10.25195/ijci.v49i2.432

Saber, O., & Mazri, T. (2021). Smart City Security Issues: The Main Attacks and Countermeasures. The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, 465–472. https://doi.org/10.5194/isprs-archives-xlvi-4-w5-2021-465-2021

Satterthwaite, D. (2007). The transition to a predominantly urban world and its underpinnings. iied.

Scandizzo, P. L., & Knudsen, O. K. (2024). The New Normalcy and the Pandemic Threat: A Real Option Approach. Journal of Risk and Financial Management, 17(2), 72. https://doi.org/10.3390/jrfm17020072

Shahidehpour, M., Li, Z., & Ganji, M. (2018). Smart cities for a sustainable urbanization: Illuminating the need for establishing smart urban infrastructures. IEEE Electrification Magazine, 6(2), 16–33. https://doi.org/10.1109/mele.2018.2816840

Shahzad, F., Javed, A. R., Zikria, Y. B., et al. (2021). Future smart cities: requirements, emerging technologies, applications, challenges, and future aspects. TechRxiv.

Sharma, R., & Arya, R. (2022). Security threats and measures in the Internet of Things for smart city infrastructure: A state of art. Transactions on Emerging Telecommunications Technologies, 34(11). Portico. https://doi.org/10.1002/ett.4571

Shawe, R., & McAndrew, I. R. (2023). Increasing Threats to United States of America Infrastructure Based on Cyber-Attacks. Journal of Software Engineering and Applications, 16(10), 530–547. https://doi.org/10.4236/jsea.2023.1610027

Silasai, O., & Khowfa, W. (2020). The study on using biometric authentication on mobile device. NU Int. J. Sci, 17, 90-110.

Silva, B. N., Khan, M., & Han, K. (2018). Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities. Sustainable Cities and Society, 38, 697–713. https://doi.org/10.1016/j.scs.2018.01.053

Singh, P., Acharya, B., & Chaurasiya, R. K. (2021). Lightweight cryptographic algorithms for resource-constrained IoT devices and sensor networks. Security and Privacy Issues in IoT Devices and Sensor Networks, 153–185. https://doi.org/10.1016/b978-0-12-821255-4.00008-0

Singh, S. K., Azzaoui, A. E., Choo, K. K. R., et al. (2023). Articles A Comprehensive Survey on Blockchain for Secure IoT-enabled Smart City beyond 5G: Approaches, Processes, Challenges, and Opportunities. Hum Centric Comput. Inf. Sci, 13, 51.

Singh, S., Sharma, P. K., Yoon, B., et al. (2020). Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city. Sustainable Cities and Society, 63, 102364. https://doi.org/10.1016/j.scs.2020.102364

Siripurapu, S., Darimireddy, N. K., Chehri, A., et al. (2023). Technological Advancements and Elucidation Gadgets for Healthcare Applications: An Exhaustive Methodological Review-Part-I (AI, Big Data, Block Chain, Open-Source Technologies, and Cloud Computing). Electronics, 12(3), 750. https://doi.org/10.3390/electronics12030750

Sizov, N. (2024). Securing Organizational Assets: A Comprehensive Analysis of Privileged Access Management. Theseus.

Smart, C. (2024). Studies in Energy, Resource and Environmental Economics. Springer International Publishing.

Sodiq, A., Baloch, A. A. B., Khan, S. A., et al. (2019). Towards modern sustainable cities: Review of sustainability principles and trends. Journal of Cleaner Production, 227, 972–1001. https://doi.org/10.1016/j.jclepro.2019.04.106

Sooriyaarachchi, J., Seneviratne, S., Thilakarathna, K., et al. (2021). MusicID: A Brainwave-Based User Authentication System for Internet of Things. IEEE Internet of Things Journal, 8(10), 8304–8313. https://doi.org/10.1109/jiot.2020.3044726

Stratigea, A., Papadopoulou, C. A., & Panagiotopoulou, M. (2015). Tools and Technologies for Planning the Development of Smart Cities. Journal of Urban Technology, 22(2), 43–62. https://doi.org/10.1080/10630732.2015.1018725

Syed, A. S., Sierra-Sosa, D., Kumar, A., et al. (2021). IoT in Smart Cities: A Survey of Technologies, Practices and Challenges. Smart Cities, 4(2), 429–475. https://doi.org/10.3390/smartcities4020024

Tahirkheli, A. I., Shiraz, M., Hayat, B., et al. (2021). A Survey on Modern Cloud Computing Security over Smart City Networks: Threats, Vulnerabilities, Consequences, Countermeasures, and Challenges. Electronics, 10(15), 1811. https://doi.org/10.3390/electronics10151811

Tahmasebi, M. (2024). Beyond Defense: Proactive Approaches to Disaster Recovery and Threat Intelligence in Modern Enterprises. Journal of Information Security, 15(02), 106–133. https://doi.org/10.4236/jis.2024.152008

Telo, J. (2023). Smart city security threats and countermeasures in the context of emerging technologies. International Journal of Intelligent Automation and Computing, 6(1), 31-45.

Törngren, M., & Grogan, P. T. (2018). How to Deal with the Complexity of Future Cyber-Physical Systems? Designs, 2(4), 40. https://doi.org/10.3390/designs2040040

Ullah, A., Anwar, S. M., Li, J., et al. (2023). Smart cities: the role of Internet of Things and machine learning in realizing a data-centric smart environment. Complex & Intelligent Systems, 10(1), 1607–1637. https://doi.org/10.1007/s40747-023-01175-4

Valencia Rojas, A. L. (2023). The Rise of Net-States in the Cyberspace: Cyber Power Dynamics and the Disruption of International Security [Master's thesis]. Charles University.

Varghese, B. (2024). Examining the Transformation of IT Departments Post-adoption of Cloud Computing Services [PhD thesis] Dublin Business School.

Vimala, H. S., et al. (2023). A systematic survey on content caching in ICN and ICN-IoT: Challenges, approaches and strategies. Computer Networks, 233, 109896. https://doi.org/10.1016/j.comnet.2023.109896

Vitunskaite, M., He, Y., Brandstetter, T., et al. (2019). Smart cities and cyber security: Are we there yet? A comparative study on the role of standards, third party risk management and security ownership. Computers & Security, 83, 313–331. https://doi.org/10.1016/j.cose.2019.02.009

Waseem, M., Adnan Khan, M., Goudarzi, A., et al. (2023). Incorporation of Blockchain Technology for Different Smart Grid Applications: Architecture, Prospects, and Challenges. Energies, 16(2), 820. https://doi.org/10.3390/en16020820

Winn, J., & Govern, K. (2009). Identity theft: Risks and challenges to business of data compromise. Temp. J. Sci. Tech. & Envtl. L., 28, 49.

Xenofontos, C., Zografopoulos, I., Konstantinou, C., et al. (2022). Consumer, Commercial, and Industrial IoT (In)Security: Attack Taxonomy and Case Studies. IEEE Internet of Things Journal, 9(1), 199–221. https://doi.org/10.1109/jiot.2021.3079916

Xia, L., Semirumi, D. T., & Rezaei, R. (2023). A thorough examination of smart city applications: Exploring challenges and solutions throughout the life cycle with emphasis on safeguarding citizen privacy. Sustainable Cities and Society, 98, 104771. https://doi.org/10.1016/j.scs.2023.104771

Xia, Z., Wu, J., Wu, L., et al. (2021). A Comprehensive Survey of the Key Technologies and Challenges Surrounding Vehicular Ad Hoc Networks. ACM Transactions on Intelligent Systems and Technology, 12(4), 1–30. https://doi.org/10.1145/3451984

Yang, P., Xiong, N., & Ren, J. (2020). Data Security and Privacy Protection for Cloud Storage: A Survey. IEEE Access, 8, 131723–131740. https://doi.org/10.1109/access.2020.3009876

Yang, W., Wang, S., Sahri, N. M., et al. (2021). Biometrics for Internet-of-Things Security: A Review. Sensors, 21(18), 6163. https://doi.org/10.3390/s21186163

Zamponi, M. E., & Barbierato, E. (2022). The Dual Role of Artificial Intelligence in Developing Smart Cities. Smart Cities, 5(2), 728–755. https://doi.org/10.3390/smartcities5020038

Zanaj, E., Caso, G., De Nardis, L., et al. (2021). Energy Efficiency in Short and Wide-Area IoT Technologies—A Survey. Technologies, 9(1), 22. https://doi.org/10.3390/technologies9010022

Zhou, W., Jia, Y., Peng, A., et al. (2019). The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved. IEEE Internet of Things Journal, 6(2), 1606–1616. https://doi.org/10.1109/jiot.2018.2847733

Zhuang, H., Zhang, J., C. B., et al. (2020). Sustainable Smart City Building Construction Methods. Sustainability, 12(12), 4947. https://doi.org/10.3390/su12124947