Journal of Systemics, Cybernetics and Informatics (2023) 21(3), 56-62
https://doi.org/10.54808/JSCI.21.03.56

A Review on Security and Privacy of Smart Cities

Abdulhakim ALSAIARI
Department of Electrical Engineering and Computer Science
Florida Atlantic University
Boca Raton, FL, USA

Mohammad ILYAS
Department of Electrical Engineering and Computer Science
Florida Atlantic University
Boca Raton, FL, USA

ABSTRACT[1]

Smart cities are expected to provide better services to citizens and urban environments, and to enhance the quality of their daily life. By utilizing smart technologies, Smart cities can deal with the emerging urbanization issues and promote sustainable development. Despite this, security and privacy issues are considered an obstacle which can impact the success of such emerging technologies and smart systems in smart cities. However, to fully leverage the benefits of smart systems and promote their further development, it's imperative to understand the security and privacy threats that weaken systems and make them vulnerable to be attacked. Motivated by these factors, this literature review provides a useful comprehensive combination of related literatures on smart cities challenges by technically analyzing various results. This review also discusses several components of smart cities such as transportation, governance, people, living, economy, innovative architecture, and associated knowledge and ideas. This paper also aims to critically examine various existing and deploying security and privacy protection methods for smart cities. Finally, we highlight several unresolved challenges and suggest future research possibilities and current security requirements, which may help building secured, privacy-protected, and stable smart cities.

Keywords: Smart city, Internet of Things, security, privacy.

1. INTRODUCTION

A smart city refers to a model comprising of technology and communication that aims at utilizing it in the development, deployment, and promotion of sustainable development activities to deal with the emerging urbanization issues [1]. A more significant percentage of the model is made up of smart network of integrated machines and objections responsible for data transmission via the cloud. Due to Internet of Things (IoT) solutions, smart cities are not extended a dream as most are now operational and expanding rapidly. These applications can obtain, examine, and oversee data on a real-time basis to enable the residents of these cities to realize improved quality of life [2]. Smart cities are also characterized by the ability of citizens to interact with various ecosystems via multiple ways utilizing mobile devices, cars, and even homes. The apparatus and the information are connected to the city's physical infrastructure and services, which play an essential role in reducing costs and enhancing sustainability [3]. Communities can also benefit from improved air quality, enhanced energy distribution, reduced traffic congestion, and enhanced trash collection due to the role of IoT. Generally, the world needs smart cities due to multiple factors. However, the main reason is that urbanization continues to expand daily as more people live in cities. Alongside the general population growth, urbanization is expected to result in billions of people in the cities within the next few decades [4]. As a result, there is a need to ensure the economic, environmental, and social sustainability factors can keep up with this form of expansion.

As smart cities are expected to bring solutions to urbanization issues, security and privacy continue to present significant challenges due to urban safety, associated with multiple threats and situations such as natural disasters, crime, and terrorism, among other challenges. Therefore, the design of a smart city must consider the processes and technologies essential for protecting and securing citizens. This is achieved through various elements, including shared communications and intelligence, operational management activities for responding and mitigating incidents, and utilization of

[1] I would like to express my deeply felt gratefulness to Professor Mohammad Ilyas for his comprehensive and detailed peer-editing of this document, as well as for his gentle alerts with regards to some important issues that they did not cross my mind when writing this document.

emerging technologies to realize physical and Cybersecurity [5]. Further, it requires collaboration and understanding between various stakeholders, including the government, and civic leaders. Security, and privacy are significant concepts in smart cities as they are more likely to continue to grow. As a result, various scholars have explored these concepts, mainly suggesting approaches for securing smart cities and addressing existing privacy issues. The literature review aims to examine the idea of security and privacy related to smart cities. By analyzing and managing the actual results from current research on challenges connected to smart cities from technological viewpoint, this paper offering a comprehensive combination of related literatures. This review also focuses on various elements of smart cities, including transportation, living, environment, people, governance, innovative architecture, and associated knowledge and ideas. The paper also focuses on how smart cities may be aligned with lengthy development goals. This comprehensive study sheds light on the fundamental underlying research subjects in smart cities, outlining existing advancements' shortcomings as well as possible future possibilities.

2. OVERVIEW OF SMART CITIES

With the emergence of smart cities as the future of urban life, various studies have explored their infrastructure, technologies utilized, and their implications. According to Ismagilova et al. [6], Smart cities utilize technology to improve their inhabitants' value of life, the environment, transportation, traffic management, the economy, and administration involvement. Smart cities have gained substantial consideration from scholars in various fields, due to the relevance of smart cities to multiple participants and the advantages and limitations associated with their implementation [6]. Silva et al. [7] described the concept of a smart city as based on the IoT. Constant population expansion and urbanization have heightened the need for novel approaches to urbanization that have minimum impact on the environment, citizen lives, and government [7]. The early adoption of ICT in city operations sparked the notions of digital cities. Later, the IoT spawned smart cities, which intelligently backing city processes with minimum human input [7]. Smart cities have evolved to solve the problems with rapid urbanization and population expansion. However, because of multiple challenges, the concept of smart cities remains not fully implemented across the world.

Lai et al. [1] identified the various technical standards of intelligent cities. According to the authors in the article, smart cities use expertise and information to improve efficiency, economic growth, biodiversity, and living standards for city dwellers. Sustainable technologies invariably promote smart city growth, notably in energy, transportation, and health [1]. The proposed system is broad, and standards are established to perfect it. Means are utilized to assist control the way smart cities operate and contribute to what a smart city implies. To foster societal growth, smart cities should be officially recognized by state and global authorities and administrations [1]. The authors suggest that while smart cities are the subject of several research and review publications, technical standards, on the other hand, are rarely explored in the present literature. Allam and Dhunny [8] studied smart cities, big data, and artificial intelligence. According to the study, cities increasingly resort to specialized technology to solve concerns such as society, environment, and morphology. In summary, Smart cities as a novel knowledge that endorses sensors and big data through the IoT, strongly supports this opportunity. This massive availability of data provides new possibilities in smart city development and administration, and most importantly new business opportunities [8]. Although big Data processing using AI may significantly contribute to the sustainability and livability in the urban, it must not be disregarded in favor of technological considerations. Visvizi and Lytras [9] explored how megacities have been transformed into smart villages due to smart city technology. Based on the findings from the article, the authors suggest that smart cities study can contribute to megacities, cities, and smart villages. The concepts of policymaking, strategy, and, eventually, the government are all pushed to the fore [9]. Considering this, it is stated that smart cities studies should be founded on real-world involvements of people living in rural and urban areas and reflect and ensure their input into policymaking and policy-design developments.

3. SMART DEVICES, SENSORS, AND TECHNOLOGIES IN SMART CITIES

To understand the significance of security and privacy of smart cities, it is essential to understand the various components that make up smart cities and their roles. Sookhak et al. [10] defined a smart city as applying multiple technologies, resources, and applications in an intelligent and coordinated approach to realize more integrated, habitable, and sustainable urban centers. The authors in the article suggest that smart cities have various applications in modern-day society, including facilitating intelligent energy optimization, smart building, smart mobility, smart governance, smart security, and smart healthcare. Ahad et al. [11] examined the various enabling technologies essential for realizing sustainable smart cities. The article specifically identifies sensors and actuators, which are part of smart devices to be the core of smart cities, especially in their role toward facilitating effective decision making. These devices have Microcontrollers that are programmed to carry out decisions depending on the information they obtain from the sensor [11]. This is achieved through embedded technologies, including wireless sensor networks, artificial intelligence, the Internet of Things (IoT), and protocols. Various kinds of literature have also identified IoT as one

of the essential technologies in smart cities. Lv et al. [3] confirmed this by suggesting that smart cities fully utilize IoT, particularly in optimizing urban management and services. Sikder et al. [2] identified various smart devices, including smart locks, smartphones, smart watches, and smart lights. These devices, among others, are prevalent in smart cities are characterized by advanced capabilities, the ability to interact with other devices and carry out multiple tasks. One of the most common components in these devices is sensors. According to Sikder et al. [2], most smart devices by default have various sensors, including light sensors, accelerometers, microphones, and gyroscope. Smart devices utilize them in achieving seamless interaction with the physical world. Rahouti et al. [12] supported this by suggesting smart devices ranging from wearable equipment, control systems, sensors, onboard units are integrated to realize a common communication platform on which smart cities run. According to Sikder et al. [2], these devices associated with smart cities have recently become prevalent due to significant growth in the use of IoT, which has given smart devices improved capabilities of interacting with other devices as human beings and the surrounding physical environment. For instance, they have allowed the seamless connection between the physical world and the devices [3]. According to the authors in Sikder et al. [2], the use of sensors in smart devices is essential in realizing features such as automation, self-learning, and context awareness. They are essential in utilizing smart devices in home appliances, personal healthcare, and even industrial applications [2]. Rahouti et al. [12] supported this by suggesting that through the wide application of smart sensors and actuators, smart cities can realize physical and cyberspaces and multiple distributed systems and services through sophisticated relationships with other systems. Therefore, smart cities comprise multiple application components ranging from smart transportation, smart education, and smart health [13]. As a result, the popularity and use of devices have led to the significant application of devices at a higher rate. Based on the report by Forbes, there will be about 3.5 billion smart devices by the year 2024 [12]. Rahouti et al. [12], went ahead to suggest that smart cities tend to be dependent on information connection and process platforms to users with services. Therefore, an advanced networking service platform is also an important component of smart cities as it is essential in ensuring smart services are rendered.

4. OVERVIEW OF SECURITY AND PRIVACY IN SMART CITIES

Various studies have explored the concept of security and privacy from the perspective of smart cities. According to Rahouti et al. [12], security is a critical requirement in networking environments, including smart cities. It allows for ensuring that the information is maintained and delivered attains the agreeable level, especially during attacks and failures. Sikder et al. [2] suggested that while the utilization of sensors in smart devices has resulted in improved functionality of the devices, it has also presented significant security challenges. For instance, sensors can launch attacks on applications and devices. The authors cite an example of how there have been various recent attempts to exploit the security of smart devices by leveraging their sensors [2]. Attackers can take advantage of sensors to transfer malicious code or activated malware already in the device, collect personal information or even capture critical information such as encryption and decryption keys between devices. According to Cui et al. [14], the creation of smart applications has also presented multiple security and privacy issues mainly due to vulnerabilities associated with every layer of a smart system [14]. Further, the various forms of attacks, including denial of services, unauthorized access, and Sybil, often affect the quality of intelligent services. The authors in Cui et al. [14] cite an example in Ukraine where approximately 230,000 residents were affected by a long-term shortage of electricity resulting from the power grid system being attacked by malicious attackers. Apart from the various forms of attacks, the collection of unnecessary information by third parties and service provides also poses privacy threats. Cui et al. [14] suggested that despite multiple protection methods, including anonymity, encryption, and biometrics, which are utilized in various fields, these approaches are not operative enough within the smart city setting. One of the reasons cited by authors on this is that most of the devices and sensors utilized within smart cities tend to have less computational power. Therefore only limited cryptography algorithms are utilized [14]. As a result of these unsuccessful measures, grave threats are posed to the systems in general. Further, smart applications' scalability, heterogeneity, and dynamic features of IoT systems also present significant privacy and security risks. The authors in Cui et al. [14] also suggest that with the continued advancement of data mining and machine learning technologies, it has become easier for attackers to bypass the existing attack detection mechanisms easily.

Sookhak et al. [10] explored the security requirements of smart cities. According to the article, although smart cities have resulted in an easier life and played a role in allowing for management and control of the various aspects of the environment, the continued increase in connectivity, complexity and interdependencies have resulted in more vulnerable smart cities in terms of privacy and security attacks [10]. Further, due to limited insight into security issues and smart cities' requirements, there are high chances of unsuitable and insecure execution and implementation of smart cities experienced [10]. Al-Turjman et al. [4] suggested that considering the nature of sensitive information collected by applications utilized in smart cities, it is essential to be conscious of the security and privacy issues which may emerge, particularly while designing and implementing such applications. As a result, the authors suggest the need to focus on existing solutions on security and privacy of information collected by

applications in smart cities, including focusing on performance improvement in future research.

5. SECURITY AND PRIVACY RISKS, THREATS, AND VULNERABILITIES IN SMART CITIES

According to Braun et al. [15], smart cities are associated with various challenges such as protecting privacy, especially in high dimensional data, utilizing artificial intelligence, ensuring the security of networks, especially those with higher attack surface, and facilitating trustworthiness in data sharing activities. These security and privacy challenges occur despite the role of smart cities in facilitating improved higher quality of life to the populations while promoting accessibility and efficiency within the cities [15]. Failure to address these issues will result in the various advantages realized from smart cities not being realized. Concerning the security and privacy of smart cities, Chen et al. [5] suggested that while smart cities have resulted in multiple changes which aim at transforming people's lives, they have also been responsible for the dangers of cyber securing such as cyber-attacks and information leakage. As a result of these dangers, the authors in the article suggest that the current Cybersecurity development cannot cope with the global smart city technologies [5]. Sookhak et al. [10] concurred with sentiments from the authors in Chen et al. [5] by suggesting that despite the promising vision of smart cities as a new approach for optimizing resources in cities and offering enhanced facilities and quality of life, security and privacy issues still exist. The fact mainly contributes to these smart cities tend to comprise various components ranging from powerful data centers, sensing devices, databases, and networks, among other components responsible for collecting, transferring, storing, and processing real-time information [10]. These components are essential for enhancing the lives of citizens in various sectors ranging from energy, education, transportation, healthcare, and even decision making [10]. However, despite these multiple roles of smart cities and devices, security and privacy issues of smart cities are not addressed accordingly. Ismagilova et al. [6] suggested that the interdependence and complexity of smart cities have resulted in organizations, designers, and integrators involved in the management of the new entities associated with smart cities experiencing socioeconomic, political, and technical challenges. The article highlights how various studies on security, and privacy in smart cities have identified threats connected with smart city infrastructure and information security, particularly how personal data is managed and processed [6]. This does affect not only the data within the smart city databases but also the connection of data with new systems and sensors for the various cities, which affect privacy and security. The authors in Ismagilova et al. [6] suggest that the threats relating to data privacy and information security can result in adverse consequences. As a result, there is a need to ensure they are addressed at the initial stages of designing and developing smart cities.

Kitchin and Dodge [16] examined various risks and mitigations concerning security of smart cities. According to the authors, it is paradoxical that smart city technologies are advocated as a mechanism for addressing and managing urban risks and uncertainly mainly through the provision of service. They are still responsible for emerging vulnerabilities and threats such as various forms of criminal activity and insecurity of city infrastructure [16]. Popescul and Genete [13] also explored security-related problems concerning smart cities. Various tendencies such as industrialized hacking, hyper-connectivity, and messy complexity have resulted in smart cities being complex environments in which the existing security analysis cannot be utilized anymore [13]. As a result, urban management should focus on more trusted architecture, security and privacy protection, standardization, and network protocols. Concerning privacy risks and threats, the authors in Popescual and Genete [13] suggest that although data collected by smart things are the basis of smart cities, the data collected tends to be sensitive and collected without explicit consent. The authors go-ahead to give an example of various sensitive information collected through smart devices, which include contacts, messages, bank accounts, and personal pictures, among other various forms of information [13]. All this sensitive information tends to be collected sometimes without measures. Apart from collecting sensitive information, smart devices include normal smartphones, also contain various sensors which can capture time stamps, locations, private conversations, and movements. In most instances, these instances collect the various forms of data without the consent and insight of the owners [13]. Popescul and Genete [13] also suggest that most of the essential data collected tend not to be handled correctly, resulting in critical privacy issues. Physical security is also assured, particularly in public networks. Ross et al. [17] agreed with Popescul and Genete [13] by suggesting that IoT devices utilized in smart cities collect various forms of information through biometric authentication, including face recognition, voice modalities, and fingerprint. While these functionalities are essential for offering security and personalized experience to the user, the data they collect tend to be easily tampered with or manipulated, resulting in the security of the smart environment being affected [17].

6. SOLUTIONS TO SECURITY AND PRIVACY ISSUES IN SMART CITIES

According to Cui et al. [14], apart from identifying and highlighting key security and privacy issues in smart cities, various works of literature have also identified solutions to security and privacy in smart cities. Smart cities are supposed to improve people's quality of life, support sustainable development, and enhance the efficiency of

urban processes [11]. With so many smart technologies in place, security and privacy concerns have risen to the fore, necessitating appropriate remedies [14]. Due to smart cities' variation, scalability, and dynamic nature, specific Cybersecurity protection measures cannot be directly applied to some intelligent applications. While creating and implementing new procedures or systems, it is also vital to be cognizant of security and privacy issues [13]. An increasing number of cities worldwide have begun to establish their smart plans to address these difficulties and improve inhabitants' well-being, stimulate economic development, and administer modern cities in a sustainable and informative manner. Cisco announced a $1 billion smart city project in 2017. China is the world's most populous country, working on over 200 smart city initiatives [14]. Predictably, a city's infrastructures are embedded in billions of devices worldwide, such as mobile mobility, smart governance, automation, and smart housing, which can be mutually advantageous for people [12]. Due to the vulnerabilities that exist at each layer of a smart system, the design of these smart apps may pose several security and privacy issues [13]. Unauthorized access, Sybil, and Denial of service (DoS) attacks all can undermine the quality of the service.

One of the techniques that have been identified by literature for addressing security and privacy issues in smart cities is encryption. Encryption schemes are the foundation of confidentiality security for smart app services since they prevent untrustworthy parties from accessing data during its life cycle of storage, processing, and dissemination [5]. As a result, it is essential to consider contemporary cryptographic techniques used in smart systems in this subsection and highlight certain unique and interesting technologies. Because of their computational complexity and energy usage, methods were used to evaluate, and encryption specifications are not entirely acceptable for the source of energy devices [15]. As a result, lightweight encrypting became a prerequisite for using encryption technology in the real world. Various studies created a proposed authentication solution for an IoT situation, safeguarding edge user communications against DDoS attacks. Others have presented a unique lightweight authentication system that uses a public key encryption approach to safeguard smart city applications [7]. Even though the Blockchain tactic is a technique instead of a field, various studies have identified it as a solution to security issues in smart cities to present it due to the significant increase in interest in recent years. Various studies have confirmed the feasibility of using Blockchain in the IoT ecosystem, indicating its potential for applications in the emerging IoT ecosystem. The distributed nature of blockchain allows apps to run in a dispersed approach, which is why many blockchain-based IoT applications are so prevalent [3]. For example, a blockchain-based security architecture was developed to ensure the secure communication of smart urban devices while also improving the system's dependability and effectiveness.

Various works of literature have also identified biometrics as one of the potential solutions towards addressing key security and privacy issues in smart cities. Biometrics are commonly used to verify IoT-based systems [13]. This technology would identify the person autonomously tailored to specific biological and behavioral traits. Biometric data, faces, voices, signatures, and other biometrics are used to extract biometric data. Brainwave-based authentication is such a technique important to mention here because it can reach a high level of identification reliability while also ensuring efficiency [7]. Various works have suggested key negotiations and common authentication protocols protect users' sensitive information in storage devices.

In comparison to existing analogous systems, the unique protocol not just effectively defeats security assaults but also maintains an appropriate communication overhead and overhead. Another feature to compare is that if these bio-based technologies aren't employed properly, the chance of privacy leakage will escalate [16]. Furthermore, privacy-preserving biometric techniques must be developed. Researchers also stated that biometrics have a bright future in these other industries, including e-business. Machine learning techniques have been used to improve intrusion detection systems' efficiency. One of the most compared Cybersecurity infrastructures to defend networks from attacks based on the actual conditions [3]. Wireless sensor networks, a vital part of the smart environment, are gaining popularity.

Various benefits of using Machine Learning technology to safeguard smart cities were identified in the comprehensive review, which included reviewing different ML techniques. During studies, a machine-based technique for secure information sensing and fusion in Whashas was also proposed. Furthermore, a recent study created a unique extraction of features and a selected model with high detection accuracy for attacks in Wi-Fi systems [13]. Several consumer ML techniques have been employed in the latest days to assess, anticipate, and make tailored judgments, in addition to security solutions. Sensor nodes and cellphones quickly develop, posing several security and privacy issues for residents. SVM may also be used to develop a complete smartphone verification system. The main concept was to learn about users' behavior patterns and how their surroundings influenced them. Researchers have also built a revolution authorization mechanism for a mobile selected model with pets based on ML technology. However, it has a widespread issue: the data utilized for analysis cannot eliminate user subjectivity, and it may not accurately represent the reality in a different IoT setting [9]. As we've seen, most defense methods can be bolstered by machine learning algorithms. Several studies have used machine learning to provide a game-theoretic model for detecting and preventing breaches in WSNs. Various kinds of literature have also assessed the current state of fingerprint

security systems from the viewpoint of adversarial ML. A detailed review undertaken by numerous studies in data mining (DM) revealed that large amounts of data obtained by the many sensors Users' smartphones and other gadgets are now being utilized to extract new legislation and knowledge to give improved services [5]. Nevertheless, because confidential material, such as individuals' locations and behavioral problems, might be revealed, systems raise some security and privacy issues. Certain confidentiality tools have been developed in current history to address this issue. material, such as individuals' locations and behavioral problems, might be revealed, systems raise some security and privacy issues. Certain confidentiality tools have been developed in current history to address this issue.

7. IMPLICATIONS OF THE STUDY

The review has examined existing security and privacy protection methods for smart cities. In recent years, a slew of creative countermeasures has been developed in various sectors. Unfortunately, based on the most recent risks and security needs, it's plausible to assume that more effective protection solutions are required to keep up with the increasing expansion of smart cities [4]. Based on our analysis, the following represent prospective prospects and research paths. The Internet of Things may be thought of as a network of networks that connects and integrates varied networks. More effective solutions are required to deal with the newest issues in this sort of complicated environment. Understanding malware dissemination features in IoT-based infrastructures, for example, or modeling information spread patterns in wireless sensor networks [11]. The establishment of effective preventive networks and the creation of successful preventative measures are critical.

Fog-based structures create new security problems as an emerging technology for implementing smart cities since the operating settings of distributed Fog systems are more prone to assaults than centralized clouds. Fog systems are tiny compared to Clouds, limiting their capacity to defend themselves [18]. Furthermore, Fog nodes are near end-users; they offer valuable chances to secure customers' privacy before sensitive personal data leaves the edge. As a result, smart device security in fog-based smart systems should be given a lot more thought [19]. Consumers should have the right to remove or migrate data from one service provider to another at any time in user-centric smart cities.

Furthermore, people's preferences for security and privacy must be considered, as attitudes and requirements differ from person to person [18]. Furthermore, the expanding number of privacy settings. Users will find it challenging to fit their settings with their actual preferences because of the settings. As a result, creating user-friendly protection aides that may improve the security and comfort of a variety of smart apps is promising [11]. One is to reduce the quantity of data gathered, used, and kept by IoT apps, which necessitates technological safeguards and political and governance support. The other is to figure out how to keep the amount of information gained to a minimum. Service providers may only uncover the knowledge that is confined to the scope of their core aims, and they are unable to mine any other sensitive information from individuals without their consent [9]. Even though several novel mechanisms have been established in recent years, practical implementation of some of these methods is unlikely. Only simple and weak preservation algorithms can be built due to sensors and devices' limited processing abilities and energy sources. As a result, further research is needed to produce lightweight countermeasures that decrease overhead while ensuring protection to meet the strong mobility, flexibility, dynamic, and low-cost criteria [8]. Smart applications are being discussed worldwide, and practically every government is working on smart initiatives. However, there is no universally accepted definition of architecture for a smart city. As a result, many existing security protection methods and network protocols focus on a single location, preventing them from being integrated into and shared throughout the smart city environment. As a result, further theoretical studies are required to lower the hurdles to smart city security.

8. CONCLUSIONS

In conclusion, because of its strong realistic necessity and practical foundation in a more urbanized world, the notion of a smart city has drawn increasing interest in academic and industrial disciplines over the last two decades. According to studies, more than half of the world's population today lives in cities. By 2050, it is expected that 66 percent of the world's population will live in cities, putting an undue strain on the climate, energy, environment, and living circumstances. A rising number of cities worldwide have begun to establish their smart plans to address these difficulties and improve inhabitants' well-being, stimulate economic development, and administer contemporary cities sustainably and intelligently. Predictably, a city's architecture is loaded with billions of gadgets that may benefit the inhabitants in various ways, including intelligent transportation, smart governance, health, smart buildings, and smart housing. However, because of the vulnerabilities that exist at each layer of a smart system, the design of these smart apps may pose several security and privacy issues. Unauthorized access, Sybil, and disruption of the system can compromise the quality of intelligent services.

Furthermore, over-collection of data by telecom operators and maybe some intermediaries put citizens' privacy at risk. Many security measures (such as cryptography, fingerprints, and anonymity) are extensively used in a variety of applications. However, these approaches are insufficient in a smart city setting. The fundamental reason for this is that most sensors and gadgets have minimal

processing capability, limiting them to using only rudimentary cryptographic techniques directly. Indirectly, these poor measures represent a major threat to the entire system. Furthermore, compared to traditional computer systems, IoT systems' diversity and various dynamic characteristics expose smart applications to significant security and privacy vulnerabilities. Furthermore, hackers have gotten "smarter" due to the fast development of the information technologies such as machine learning and data mining. They have gained the capacity to circumvent current attack detection systems, IoT systems' diversity and various dynamic characteristics expose smart applications to significant security and privacy vulnerabilities. Furthermore, hackers have gotten "smarter" due to the fast development of the information technologies such as machine learning and data mining. They have gained the capacity to circumvent current attack detection measures. These difficulties drive scholars to examine the currently used and developing technology for defending smart cities and offer future research possibilities for readers interested in learning more about this exciting and useful concept of smart cities.

This literature review contributes by offering a comprehensive overview of protective strategies for safeguarding smart cities from several disciplines' viewpoints, including the most recently discovered or deployed mechanisms and theories. It also assesses the availability of cutting-edge security technology for smart cities and highlights several unresolved challenges with limited viable responses. It also suggests future research possibilities relevant to existing difficulties and current security requirements, which may help build more secure, privacy-protected, and stable smart cities.

9. REFERENCES

[1] C. S. Lai *et al*., "A review of technical standards for smart cities," *Clean Technologies*, vol. 2, no. 3, pp. 290–310, Aug. 2020.

[2] A. K. Sikder, G. Petracca, H. Aksu, T. Jaeger, and A. S. Uluagac, "A survey on sensor-based threats and attacks to smart devices and applications," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 1125–1159, 2021.

[3] Z. Lv, L. Qiao, A. Kumar Singh, and Q. Wang, "AI-empowered IoT security for smart cities," *ACM Transactions on Internet Technology*, vol. 21, no. 4, pp. 1–21, Jul. 2021.

[4] F. Al-Turjman, H. Zahmatkesh, and R. Shahroze, "An overview of security and privacy in smart cities' IoT communications," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 3, Jul. 2019.

[5] D. Chen, P. Wawrzynski, and Z. Lv, "Cyber security in smart cities: A review of deep learning-based applications and case studies," *Sustainable Cities and Society*, vol. 66, p. 102655, Dec. 2021.

[6] E. Ismagilova, L. Hughes, N. P. Rana, and Y. K. Dwivedi, "Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework," *Information Systems Frontiers*, vol. 24, pp. 393–414, Jul. 2020.

[7] B. N. Silva, M. Khan, and K. Han, "Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities," *Sustainable Cities and Society*, vol. 38, pp. 697–713, Apr 2018.

[8] Z. Allam and Z. A. Dhunny, "On big data, artificial intelligence and smart cities," *Cities*, vol. 89, pp. 80–91, Jun. 2019.

[9] A. Visvizi and M. D. Lytras, "Rescaling and refocusing smart cities research: from mega cities to smart villages," *Journal of Science and Technology Policy Management*, vol. 9, no. 2, pp. 134–145, Jul. 2018.

[10] M. Sookhak, H. Tang, Y. He, and F. R. Yu, "Security and privacy of smart cities: A survey, research issues and challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1718–1743, Aug. 2018.

[11] M. A. Ahad, S. Paiva, G. Tripathi, and N. Feroz, "Enabling technologies and sustainable smart cities," *Sustainable Cities and Society*, vol. 61, no. 102301, Oct. 2020.

[12] M. Rahouti, K. Xiong, and Y. Xin, "Secure software-defined networking communication systems for smart cities: Current status, challenges, and trends," *IEEE Access*, vol. 9, pp. 12083–12113, 2020.

[13] D. Popescul and L. D. Genete, "Data Security in Smart Cities: Challenges and Solutions," *papers.ssrn.com*, vol. 20, pp. 29–38, 2016.

[14] L. Cui, G. Xie, Y. Qu, L. Gao, and Y. Yang, "Security and privacy in smart cities: Challenges and opportunities," *IEEE Access*, vol. 6, pp. 46134–46145, 2018.

[15] T. Braun, B. C. M. Fung, F. Iqbal, and B. Shah, "Security and privacy challenges in smart cities," *Sustainable Cities and Society*, vol. 39, pp. 499–507, May. 2018.

[16] R. Kitchin and M. Dodge, "The (in)security of smart cities: Vulnerabilities, risks, mitigation, and prevention," *Journal of Urban Technology*, vol. 26, no. 2, pp. 47–65, 2019.

[17] A. Ross, S. Banerjee, and A. Chowdhury, "Security in smart cities: A brief review of digital forensic schemes for biometric data," *Pattern Recognition Letters*, vol. 138, pp. 346–354, Oct. 2020.

[18] A. Khakimov, A. A. Ateya, A. Muthanna, I. Gudkova, E. Markova, and A. Koucheryavy, "IoT-fog based system structure with SDN enabled," in Proceedings of the 2nd International Conference on Future Networks and Distributed Systems, Jun. 2018, pp. 1–6.

[19] G. George and S. Sankaranarayanan, "Light weight Cryptographic solutions for Fog Based Blockchain," in *2019 International Conference on Smart Structures and Systems (ICSSS)*, 2019, pp. 1–5.