2023 IEEE International Conference on Emerging Trends in Engineering, Sciences and Technology (ICES&T) | 978-1-6654-5560-2/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICEST56843.2023.10138843

Cybersecurity and Smart Cities: Current Status and Future

Muhammad Yasir Habib
Dept. of Electronic Engineering
Faculty of Engineering
The Islamia University of Bahawalpur
Pakistan
yasir.4526@gmail.com

Haseeb Ahmad Qureshi
Dept. of Computing and Informatics
Faculty of Computing
Bournemouth University
Bournemouth, United Kingdom
haseebahmad89@gmail.com

Shujahat Ali Khan
College of Engineering, IT and Environment
Charles Darwin University
Darwin, Australia
shujahatkhan345@gmail.com

Zara Mansoor
Dept. of Software Engineering
Faculty of Computing
The Islamia University of Bahawalpur
Bahawalpur, Pakistan
zara.mansoor@iub.edu.pk

Abdul Rehman Chishti
Dept. of Information and Communication Engineering
Faculty of Engineering
The Islamia University of Bahawalpur
Bahawalpur, Pakistan
rehman.chishti@iub.edu.pk

***Abstract*—A Smart city implements the latest IoT and information and communication technologies (ICT) to improve the quality of urban city administrations, decrease expenditures, asset management and interconnect citizens of a Smart city. Smart cities offer numerous advantages like improved energy productivity, management, healthcare facilities, efficient transport systems, proper waste and water management, and individual security. Nonetheless, this reliance on ICT and IoT technologies makes a Smart city prone to digital cyber assaults. These technologies are vulnerable to many security issues like Information theft, Eavesdropping attack, Denial of service, Communication delays, Data manipulation, IoT security attacks, Communication interception, Jamming, Sensor failure, insecure API, and Remote exploitation. This research study intends to address opinions on cybersecurity technologies, vulnerabilities, and cybercrime awareness based on the systematic literature review "PRISMA Model" as our research method and help researchers and practitioners to look for innovative Smart City solutions. Our research endeavors to momentarily depict the central ideas of digital security and protection issues related to Smart city areas and uncover digital cyber-attacks that focus on Smart city communities in the literature. In brief, the focus of this research is to explore and review the aspects of Smart city cybersecurity issues, Smart city vulnerabilities related to information security, and provide a comprehensive research framework that will help the researchers and practitioners explore this area of research.**

***Index Terms*—Smart Cities, Cybersecurity, Systematic Review, PRISMA Model, Vulnerabilities, Cybersecurity challenges.**

I. Introduction

Smart cities correspond to cities that use the latest technologies like ICT infrastructure, automated services, cloud computing, and IoT-enabled technologies for improved quality of services to improve the quality of life for the citizens of such cities [1]. The improvement in the systems of health, transportation and the local economy improves the quality of life of the residents. Smart cities present exceptional comforts and improve personal satisfaction, effective business activity, rapid transportation, secure monetary exchange and logically instructive exploration [2]. A complex and sophisticated network of interconnected devices, sensors and programmed software is implemented and managed [3]. Smart cities will be developed after the deployment of Smart governance systems, Smart mobility systems, Smart living, Smart Economy, Smart grid systems, Smart Business and Smart homes [4]. In Smart cities, systems are embedded to exchange data and people are well-informed about their local surroundings. Cybersecurity in a Smart city has been a concern for Governments, researchers, and practitioners. There is a need to take corrective decisions in public administration while planning and to implant a Smart city [5]. It is crucial to make technological decisions while implementing a smart city infrastructure and its administrative decisions. A smart city infrastructure needs to have the best policies at the government level, proper legislation, and take care of digital security. Setting up a smart city without taking measures about digital security and privacy concerns is a nutshell for citizens, government, and resources [6]. Therefore, sufficient planning of smart city infrastructure is a basic need before setting up a smart city. Figure 1 illustrates the key elements of smart city infrastructure.

The exponential growth in the development of Smart cities with their incorporated technologies has carried us into the world of modern cybersecurity challenges [7] . The security of smart city deployments is a critical challenge and has been the utmost concern after the exponential growth in the development of smart cities with their incorporated ICT infrastructure and IoT technologies. Smart city technologies are vulnerable to many security issues like information theft, Eavesdropping attack, Denial of service, the introduction of communication delays, Data manipulation, IoT security attacks, Communica-

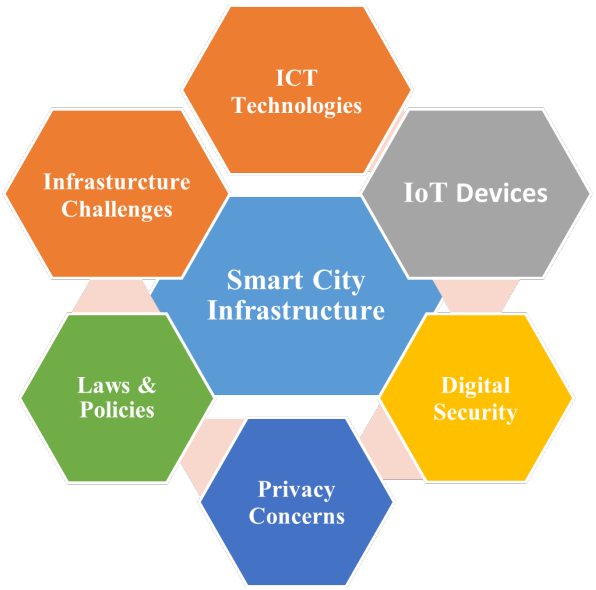

Fig. 1. A Smart City Infrastructure

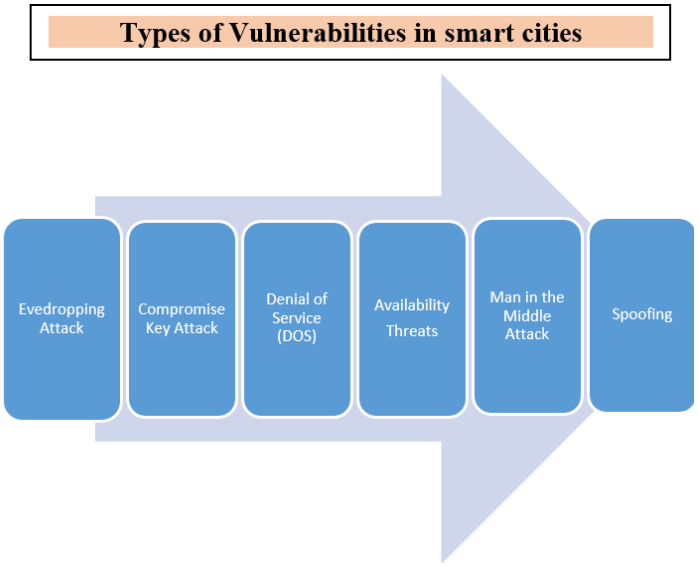

Fig. 2. Type of Vulnerabilities in Smart Cities.

tion interception and jamming, sensor failure, insecure API and remote exploitation [8]. Therefore, there is a need for persistent and robust security strategies to cope with such security threats and vulnerabilities associated with Smart system deployments [9]. Relying on the ramifications of new advancements, different parts of security could get exposed [10]. The security challenges attracted many researchers and researchers to suggest some strategies to cope with these challenges. Various cryptographic algorithms, biometric identification, face recognition, machine learning, game theory, Data mining, and Blockchain technology exist for the security of Smart systems deployed in Smart cities [11]. The focus of this research is to explore and review the aspects of smart cities like cybersecurity issues, identification of vulnerabilities and threats related to information security in smart cities, and provide a comprehensive and effective research framework that will help the researchers and practitioners to explore this area of research as shown in Figure 2.

In this paper, The design ideas of a Smart City and briefly reviewed ongoing Smart city activities, initiatives and undertakings are critically discussed. After distinguishing a few digital security vulnerabilities of Smart Cities, different protection and security arrangements, proposals, and guidelines for smart cities are presented in detail. It is discovered that it is crucial to make rules, systems, and proper infrastructures for the cybercrime issues in smart cities to make all these technologies beneficial.

The structure of the rest of this paper is as follows. Section II details the literature review that helps us research the cyber vulnerabilities in Smart Cities and multiple existing approaches to get insights into the various aspects of cyber issues. Section III describes the complete Research Methodology that focuses systematic literature review using PRISMA Model. PRISMA Model for the systematic literature review helped us to undertake extensive and relevant research studies. In section IV, the conclusion based on the extensive literature research has been drawn. Section V gives us the future insights and impact of this research paper.

II. Literature Review

During the past twenty years, the concept of "smart city" has pulled attraction in expanding consideration in both academia and industries because it has a solid reasonable necessity and viable foundation in an undeniably urbanized world [12]. The term 'smart city' is a broad and questionable term, with no concurred definition or agreement on how urban communities should move towards the plan. Various smart city definitions are proposed by researchers and practitioners; some have a wide spotlight while others revolve around innovation and information or residents [13].

According to Khatoun R. and Zeadally, S., smart cities are meant to improve the daily life of people, focuses on the sustainable development of cities, and enhance the usefulness of metropolitan frameworks [14]. A smart city is a city that utilizes inventive advances to offer types of assistance and take care of city issues. The significant concern is offering outstanding quality assistance for the residents to improve their standard of living [15]. Smart cities use the latest ICT and IoT-based technologies to transform traditional infrastructures into smarter and more efficient infrastructures that provide reliable communication, resource-effective environment and facilitated city-relevant modernized urban environments [16]. This idea of smart cities is gradually coming into reality as numerous nations all around the planet are receiving this thought and thinking of their model of Smart City communities. The exponential growth of the Internet of Things (IoT) gadgets uncovers the wide range of vulnerabilities where digital hackers and pernicious entertainers can cause our digital security and privacy. IoT and Artificial intelligence play a significant

role in urban city arrangement, advancement, and management with the development of security frameworks, traffic checking, and social order management with access and control of their home. All these factors are making the living experience of Smart city residents living experience better and better [17]. Smart city deployments are meant to enhance productivity, profitability and efficiency but there is a serious challenge in order to maintain security and communication. There are the serious risks for cyber threats that can negatively impact in a great deal for the citizens and authorities of smart cities. According to Adel S. Elmaghraby, there are two significant and shared challenges: security and privacy [18]. Security incorporates illicit admittance to data and assaults making actual disturbances in service accessibility. Privacy ensures frameworks that assemble information and trigger suitable and emergent response when required confidently. The execution of secure and private frameworks are fundamental for a Smart City in which the citizens would like to live [19].

The new era of technology has presented the solution to city security problems in the form of sensor fusion, machine learning, and artificial intelligence. But this also has its own share of challenges ranging from technical to financial. As cyber-attacks fill in volume and intricacy, Artificial Intelligence (AI) is helping under-resourced security task experts stay in front of dangers. Artificial Intelligence (AI) gives instant experiences to help achieve battle through the commotion of thousands of day-by-day security threats, definitely decreasing reaction times [20]. The literature survey on a smart city has to lead us to recognize two significant areas that were named as non-technical and technical issues. In the non-technical section, the following components have a key place: planning finance and monetary challenges; business projects, cooperation, and the absence of an adequate vision of setting up a smart city, political and administration; and smart city guide, context-oriented; initiative, principles, and smart city infrastructure [21].

In the technical section of a Smart City challenges, the following aspects have a key place: Privacy and protection, digital security and interoperability. Digital security has been a debatable topic for smart city implementations. The consequences of such cyber-attacks and vulnerabilities can be quite harmful. Password cracking, social engineering on connected systems, dumping memory, access of any debug report, firmware alteration, monitoring of communication over any network, and tempering of data can be real cyber threats for any smart city. Table I gives a rundown of the challenges from a literature survey.

The security of smart city deployments is a critical challenge and has been the utmost concern after the exponential growth in the development of smart cities with their incorporated ICT infrastructure and IoT technologies. The vulnerabilities that a smart city can have are information theft, Eavesdropper's attack, Denial of Service (DOS), permanent Denial of Service (PDOS), distributed denial of service (PDOS), Man in the Middle, Device hijacking, Spoofing, Physical attack, communication delays, data manipulation, IoT security attacks, communication interception, Sensor failure, insecure API, Firmware Modification, Authorization, Compromised Access points, physical attack, Spoofing and unauthorized access to controller/sensor [22].

TABLE I
SMART CITY TECHNICAL AND NON-TECHNICAL CHALLENGES

Technical Challenges	Non- Technical Challenges
Digital Security: • Lack of adequate cryptographic Techniques. • Unprotected encryption-key Management. • Non-existent secure IoT device administrations. • weaponized AI progression by digital hackers. • Absence of assurance versus DDoS assaults. • Lack of technical expertise in human resources	**Financial Concerns:** • Poor Financial management. • Lack of funding allocated for smart city initiatives by the decision-makers. • No plan for monetizing investments. • Poor procurement management. • Delays in catching profitability by the finance management. • Inadequate performance of acting management working in smart cities.
Privacy: • Privacy of sensitive devices is always at the stack in smart cities. • Proper privacy in smart cities demands more secure surveillance. • Hackers, intruders, and hijackers can get unauthorized access. • Intruders can hack smart devices and the privacy of smart devices is compromised. • Hackers can introduce delays after unauthorized access. • Control over IoT devices by digital hackers is quite dangerous.	**Collaborative Challenges:** • Strong collaborations with important stakeholders are quite important. • It is important to devise suitable laws and policies that encourage a safe and secure smart city. • There must be a feasible environment to address issues between stakeholders. • Lack of coordination between smart city administrations. • Unstable internet connectivity. • Digital insecurity.

Cyber security in smart city deployments has been a key challenge for the successful management of smart cities. Many researchers and practitioners have proposed different methodologies to address the above-mentioned vulnerabilities. Batty and Michael proposed a distributed framework for the IoT application which guarantees the data conveyance concerning trust, protection, and security [23]. Soryal et.al, introduced an imaginative way to deal with distinguishing Denial of Service (DoS) assault, with undetectable hosts that utilized the IEEE-802.11 DCF conventions, a DoS assault attacks remote organizations [24]. Mat Tattam and co-authors reviewed a very efficient modeling known as Threat Modeling (TM) for APT attacks.

Threat Modeling (TM) is an interaction during which explicit potential security weaknesses and their related dangers are distinguished so that they can be tended to in a focused way. It is an instrument to assess controls, and framework

security and a vital assignment for creating secure applications. Threat Modelling makes and formalizes an interaction that recognizes dangers and examines the weaknesses of an individual or mix of Information and communication technologies (ICT) resources [25]. Ashok and co-authors examined cyber threats and introduced Wide-Area Monitoring, Protection and Control (WAMPAC) a hypothetical gaming way to deal which address the issue of digital actual security. They investigated the features of digital physical test beds utilized for the assessment of security [26]. Many cryptographic algorithms, biometric identification, face recognition and machine learning algorithms are also presented in the literature as the solution to digital security in a smart city [27]. The countermeasures that can address the above-mentioned vulnerabilities can be Two-factor authentication, IoT forensics, Risk and Threat model, Method of Data backup and recovery options, public key infrastructure, cryptographic algorithms, Chaotic Encryption techniques, Data leakage prevention, Awareness training for the residents of smart cities, cybercrime intelligence, Firewalls, Anti-Malware solutions and Risk Assessment technologies [28].

III. RESEARCH METHODOLOGY

Many methodologies and studies are there to discuss and review the available data for smart city security challenges. For example, Yuba Raj Panta and his co-authors presented a deliberate writing audit that depicted the innovative segments which are the integral elements of smart city challenges and a correlation of existing advancements and case studies [29].

The scope of our research studies is to explore and review the aspects of smart cities like cybersecurity issues, identification of vulnerabilities and the threats related to information security in smart cities and provide a comprehensive and effective research framework that will help the researchers and practitioners to explore in this area of research. The research study will be carried out on the concept of PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) Model in which a systematic literature review of a clearly formulated research problem is conducted in a systematic way [30].

PRISMA can be utilized to report the consequences of a methodical audit assessing the impacts of an intercession, regardless of whether the survey is restricted to randomized controlled preliminaries or incorporates different kinds of exploration. Researchers and practitioners can likewise utilize PRISMA to basically assess distributed orderly audits. The purpose of the PRISMA Statement is to assist content creators with improving the literature review of methodical audits and meta-examinations. Researchers tend to focus on randomized preliminaries, however, PRISMA can likewise be utilized as a reason for revealing methodical audits of different kinds of examination, especially assessments of intercessions [31].

Several steps are followed for our study's systematic review. These include the formulation of a question, protocol formulation, conduction of research, selection of a suitable and relevant case study, data extraction, data analysis of the provided, and at the end, interpretation of the results that are carried out. Various research articles, journals and conference publications are downloaded, narrowed down and critically reviewed to develop a fair understanding of multiple approaches related to 'Cybersecurity issues in smart cities' through an outstanding approach of review known as PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses). Our research that follows the PRISMA Model is conducted following the given steps:

A. Protocol Formulation

Finding the important but only peer-reviewed research articles related to the important keywords of our research problem from the literature [32].

B. Filtering

Filtering the research articles by its title, abstract and keywords. Prisma model is shown in Figure 3.

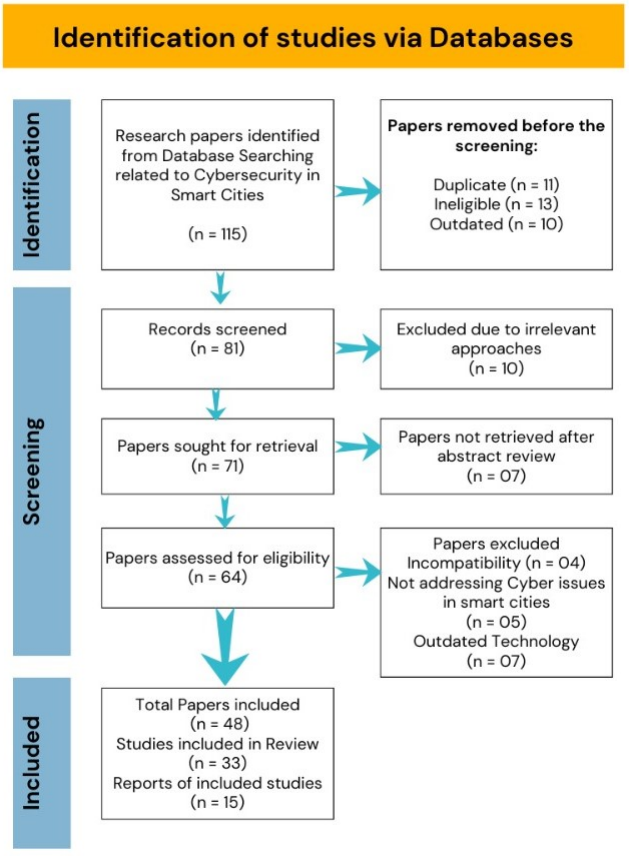

Fig. 3. PRISMA Model

C. Data Extraction

Data extraction from the chosen research articles will be carried out. The Flow chart portrays the progression of data through the various periods of a Systematic Review. It delineates the number of records distinguished, included, and prohibited, and the explanations behind avoidance.

Our Research Model i:e PRISMA Model includes the processes of the identification of peer-reviewed research articles from Database Searching related to Cybersecurity in smart cities by using relevant keywords, undergoing the screening of those downloaded papers, narrowing it down to the most relevant papers suitable for our research due to its compatibility and relevant approaches discussed in those papers.

In the context of a smart city, a rigorous literature survey is performed. We downloaded 115 research articles that were purely peer-reviewed. We analyzed their abstract and conclusion and performed the screening very keenly. After narrowing down through a systematic method of literature review, i: e PRISMA Model, we critically reviewed the final 15 research papers. The outcome that we observed after the critically evaluation of the final 15 research papers can be seen in the comparison Table II.

Many challenges and issues in smart are present in literature due to their significance and importance. Smart city services, research requirements, issues regarding policies, code visualization and future challenges are having a significant part in the literature. The importance of ever-changing challenges cannot be denied due to ever-changing technological advancements in smart cities and the cyber issues and vulnerabilities are increasing due to the developmental growth in smart systems. Below is the visual representation of some challenges relevant to smart cities and the cyber-issues in smart cities presented by researchers and authors through "CiteSpace" from 2011-2020 [33] illustrated in Figure 4.

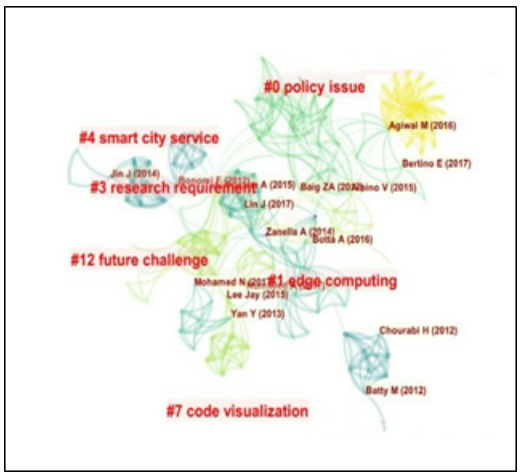

Fig. 4. CiteSpace Visualized Diagram

IV. Conclusion

Smart city areas are intended to productively oversee developing urbanization, energy utilization, keep a green climate, improve the financial and expectations for everyday comforts of their residents, and raise individuals' capacities to proficiently utilize and embrace the advanced Information and Communication Technologies (ICT). Cyber-Security in smart city areas has been a key topic for the researchers and practitioners. In this research paper, a research work following

TABLE II
Challenges comparision table

References	SC Non-Technical Challenges	SC Security Challenges	SC Privacy Challenges	Cyber Vulnerabilities	Cyber Physical Systems	IoT Based Technologies	Virtual Power Plants	Smart Governance	Smart Transportation	Cybersecurity Framework	Smart City Framework
[34]	✓	✓	✓	✓	×	×	×	✓	✓	×	×
[35]	×	✓	✓	✓	×	✓	×	×	×	✓	✓
[36]	×	✓	✓	✓	✓	✓	×	✓	×	×	✓
[37]	×	✓	×	✓	×	✓	×	×	✓	✓	✓
[38]	✓	✓	✓	✓	×	✓	×	×	✓	×	✓
[39]	×	✓	✓	✓	✓	✓	✓	×	×	✓	✓
[40]	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	✓
[41]	×	✓	✓	✓	×	✓	×	✓	✓	×	✓
[42]	×	✓	✓	✓	×	✓	×	✓	✓	×	✓
[43]	×	✓	✓	✓	✓	✓	×	×	×	✓	✓
[44]	✓	✓	✓	✓	×	✓	×	✓	×	✓	✓
[45]	×	✓	✓	✓	×	×	×	✓	✓	×	✓
[46]	×	✓	✓	✓	×	×	×	✓	✓	×	✓
[47]	×	✓	✓	✓	×	✓	×	×	×	✓	✓
[48]	×	✓	✓	✓	×	✓	×	✓	✓	✓	✓

PRISMA Model insights a detailed review of the Smart Cities around the world, some examples of implemented solutions, afterward further investigates how the security of people could be uncovered and how this openness could be relieved utilizing different protection upgrading advancements. A comprehensive review of existing security improving advances is introduced, notwithstanding their applications in the setting of smart cities. All the security issues, existing infrastructures of cyber-secured smart cities, the role of Artificial intelligence (AI) in cyber secured smart cities and existing literature already present is beautifully explained.

V. Future Work

Smart Cities are viewed as the association of physical, information and communication technology (ICT), social and business foundations to improve the general insight in city activities where knowledge and intelligence, it might be said, is the capacity to settle on impartially better choices. Joining ICT and IoT infrastructures together opens the security and privacy challenges in smart cities alongside individuals living

in them. Therefore, in future, Smart Cities can improve the quality of life of their residents by providing upgraded Smart services like digital security, comfort, less travelling time, Easy access to data, fast and accurate services, Smart Parking, Smart municipal services, Smart healthcare facilities, Smart Economy, Smart building services and many more. In future, our research will help researchers and practitioners explore new insights to make cities secure, Smart and sustainable cities.

REFERENCES

[1] J. Fan, W. Yang, and K.-Y. Lam, "Cybersecurity challenges of iot-enabled smart cities: A survey," *arXiv preprint arXiv:2202.05023*, 2022.

[2] H. Zhu, L. Shen, and Y. Ren, "How can smart city shape a happier life? the mechanism for developing a happiness driven smart city," *Sustainable cities and society*, vol. 80, p. 103791, 2022.

[3] S. E. Bibri and J. Krogstie, "The emerging data–driven smart city and its innovative applied solutions for sustainability: The cases of london and barcelona," *Energy Informatics*, vol. 3, pp. 1–42, 2020.

[4] C. S. Lai, Y. Jia, Z. Dong, D. Wang, Y. Tao, Q. H. Lai, R. T. Wong, A. F. Zobaa, R. Wu, and L. L. Lai, "A review of technical standards for smart cities," *Clean Technologies*, vol. 2, no. 3, pp. 290–310, 2020.

[5] A. R. Javed, F. Shahzad, S. ur Rehman, Y. B. Zikria, I. Razzak, Z. Jalil, and G. Xu, "Future smart cities requirements, emerging technologies, applications, challenges, and future aspects," *Cities*, vol. 129, p. 103794, 2022.

[6] R. Kitchin and M. Dodge, "The (in) security of smart cities: Vulnerabilities, risks, mitigation, and prevention," in *Smart Cities and Innovative Urban Technologies*. Routledge, 2020, pp. 47–65.

[7] E. Okai, X. Feng, and P. Sant, "Smart cities survey," in *2018 IEEE 20th international conference on high performance computing and communications; IEEE 16th international conference on smart city; IEEE 4th international conference on data science and systems (HPCC/SmartCity/DSS)*. IEEE, 2018, pp. 1726–1730.

[8] C. Reuter, J. Haunschild, M. Hollick, M. Mühlhäuser, J. Vogt, and M. Kreutzer, "Towards secure urban infrastructures: Cyber security challenges for information and communication technology in smart cities," *Mensch und Computer 2020-Workshopband*, 2020.

[9] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for internet of things (iot) security," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1646–1685, 2020.

[10] K. Kimani, V. Oduol, and K. Langat, "Cyber security challenges for iot-based smart grid networks," *International journal of critical infrastructure protection*, vol. 25, pp. 36–49, 2019.

[11] 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. 46 134–46 145, 2018.

[12] A. Kirimtat, O. Krejcar, A. Kertesz, and M. F. Tasgetiren, "Future trends and current state of smart city concepts: A survey," *IEEE access*, vol. 8, pp. 86 448–86 467, 2020.

[13] S. Parnell, "Defining a global urban development agenda," *World development*, vol. 78, pp. 529–540, 2016.

[14] R. Khatoun and S. Zeadally, "Smart cities: concepts, architectures, research opportunities," *Communications of the ACM*, vol. 59, no. 8, pp. 46–57, 2016.

[15] 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, 2018.

[16] A. Alibasic, R. Al Junaibi, Z. Aung, W. L. Woon, and M. A. Omar, "Cybersecurity for smart cities: A brief review," in *Data Analytics for Renewable Energy Integration: 4th ECML PKDD Workshop, DARE 2016, Riva del Garda, Italy, September 23, 2016, Revised Selected Papers 4*. Springer, 2017, pp. 22–30.

[17] K. T. Chui, M. D. Lytras, and A. Visvizi, "Energy sustainability in smart cities: Artificial intelligence, smart monitoring, and optimization of energy consumption," *Energies*, vol. 11, no. 11, p. 2869, 2018.

[18] A. S. Elmaghraby and M. M. Losavio, "Cyber security challenges in smart cities: Safety, security and privacy," *Journal of advanced research*, vol. 5, no. 4, pp. 491–497, 2014.

[19] O. E. Idrissi, A. Mezrioui, and A. Belmekki, "Cyber security challenges and issues of industrial control systems–some security recommendations," in *2019 IEEE International Smart Cities Conference (ISC2)*. IEEE, 2019, pp. 330–335.

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

[21] R. Sánchez-Corcuera, A. Nuñez-Marcos, J. Sesma-Solance, A. Bilbao-Jayo, R. Mulero, U. Zulaika, G. Azkune, and A. Almeida, "Smart cities survey: Technologies, application domains and challenges for the cities of the future," *International Journal of Distributed Sensor Networks*, vol. 15, no. 6, p. 1550147719853984, 2019.

[22] K. Somasundaram and K. Selvam, "Iot–attacks and challenges," *Int. J. Eng. Tech. Res*, vol. 8, no. 9, pp. 9–12, 2018.

[23] M. Batty, K. W. Axhausen, F. Giannotti, A. Pozdnoukhov, A. Bazzani, M. Wachowicz, G. Ouzounis, and Y. Portugali, "Smart cities of the future," *The European Physical Journal Special Topics*, vol. 214, pp. 481–518, 2012.

[24] J. Soryal, X. Liu, and T. Saadawi, "Dos detection in ieee 802.11 with the presence of hidden nodes," *Journal of advanced research*, vol. 5, no. 4, pp. 415–422, 2014.

[25] M. Tatam, B. Shanmugam, S. Azam, and K. Kannoorpatti, "A review of threat modelling approaches for apt-style attacks," *Heliyon*, vol. 7, no. 1, p. e05969, 2021.

[26] A. Ashok, A. Hahn, and M. Govindarasu, "Cyber-physical security of wide-area monitoring, protection and control in a smart grid environment," *Journal of advanced research*, vol. 5, no. 4, pp. 481–489, 2014.

[27] L. Yang, N. Elisa, and N. Eliot, "Privacy and security aspects of e-government in smart cities," in *Smart cities cybersecurity and privacy*. Elsevier, 2019, pp. 89–102.

[28] V. Rao and K. Prema, "A review on lightweight cryptography for internet-of-things based applications," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, pp. 8835–8857, 2021.

[29] Y. R. Panta, S. Azam, B. Shanmugam, K. C. Yeo, M. Jonkman, F. De Boer, and M. Alazab, "Improving accessibility for mobility impaired people in smart city using crowdsourcing," in *2019 Cybersecurity and Cyberforensics Conference (CCC)*. IEEE, 2019, pp. 47–55.

[30] D. Moher, L. Shamseer, M. Clarke, D. Ghersi, A. Liberati, M. Petticrew, P. Shekelle, and L. A. Stewart, "Preferred reporting items for systematic review and meta-analysis protocols (prisma-p) 2015 statement," *Systematic reviews*, vol. 4, no. 1, pp. 1–9, 2015.

[31] B. Hutton, F. Catala-Lopez, and D. Moher, "The prisma statement extension for systematic reviews incorporating network meta-analysis: Prisma-nma," *Medicina Clínica (English Edition)*, vol. 147, no. 6, pp. 262–266, 2016.

[32] S. Jalali and C. Wohlin, "Systematic literature studies: database searches vs. backward snowballing," in *Proceedings of the ACM-IEEE international symposium on Empirical software engineering and measurement*, 2012, pp. 29–38.

[33] Y.-M. Guo, Z.-L. Huang, J. Guo, H. Li, X.-R. Guo, and M. J. Nkeli, "Bibliometric analysis on smart cities research," *Sustainability*, vol. 11, no. 13, p. 3606, 2019.

[34] B. Kumar, M. AbuAlhaija, L. Alqasmi, and M. Dhakhri, "Smart cities: A new age of digital insecurity," in *2020 9th International Conference System Modeling and Advancement in Research Trends (SMART)*. IEEE, 2020, pp. 267–272.

[35] J. Curzon, A. Almehmadi, and K. El-Khatib, "A survey of privacy enhancing technologies for smart cities," *Pervasive and Mobile Computing*, vol. 55, pp. 76–95, 2019.

[36] R. Khatoun and S. Zeadally, "Cybersecurity and privacy solutions in smart cities," *IEEE Communications Magazine*, vol. 55, no. 3, pp. 51–59, 2017.

[37] S. Datta and S. Sarkar, "Automation, security and surveillance for a smart city: Smart, digital city," in *2017 IEEE Calcutta Conference (CALCON)*. IEEE, 2017, pp. 26–30.

[38] T. Jameel, R. Ali, and S. Ali, "Security in modern smart cities: An information technology perspective," in *2019 2nd International Conference on Communication, Computing and Digital systems (C-CODE)*. IEEE, 2019, pp. 293–298.

[39] S. K. Venkatachary, J. Prasad, R. Samikannu, A. Alagappan, and L. J. B. Andrews, "Cybersecurity infrastructure challenges in iot based virtual power plants," *Journal of Statistics and Management Systems*, vol. 23, no. 2, pp. 263–276, 2020.

[40] Ö. Durmus, A. Varol, and N. Varol, "Infrastructure requirements for cybersecurity," in *2019 1st International Informatics and Software Engineering Conference (UBMYK)*. IEEE, 2019, pp. 1–5.
[41] A. AlDairi *et al.*, "Cyber security attacks on smart cities and associated mobile technologies," *Procedia Computer Science*, vol. 109, pp. 1086–1091, 2017.
[42] M. A. Ahad, S. Paiva, G. Tripathi, and N. Feroz, "Enabling technologies and sustainable smart cities," *Sustainable cities and society*, vol. 61, p. 102301, 2020.
[43] K. N. Qureshi, S. S. Rana, A. Ahmed, and G. Jeon, "A novel and secure attacks detection framework for smart cities industrial internet of things," *Sustainable Cities and Society*, vol. 61, p. 102343, 2020.
[44] H. Habibzadeh, B. H. Nussbaum, F. Anjomshoa, B. Kantarci, and T. Soyata, "A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities," *Sustainable Cities and Society*, vol. 50, p. 101660, 2019.
[45] Z. A. Baig, P. Szewczyk, C. Valli, P. Rabadia, P. Hannay, M. Chernyshev, M. Johnstone, P. Kerai, A. Ibrahim, K. Sansurooah *et al.*, "Future challenges for smart cities: Cyber-security and digital forensics," *Digital Investigation*, vol. 22, pp. 3–13, 2017.
[46] S. Manickam and A. Kooy, "Internet of things for smart cities: Challenges, security and privacy issues," *Security and Privacy Issues (October 17, 2020)*, 2020.
[47] Z. Ullah, F. Al-Turjman, L. Mostarda, and R. Gagliardi, "Applications of artificial intelligence and machine learning in smart cities," *Computer Communications*, vol. 154, pp. 313–323, 2020.
[48] F. Ahmad and A. Adnane, "Article in ieee communications magazine• february 2017 ieee communications magazine," *IEEE Communiations Magazine*, pp. 16–24, 2017.