Information Security and Data Protection in Smart Cities

[1]Bhupendra Dhakrey, Research Scholar, Rama University Uttar Pradesh, Kanpur
[2]Hari Om Sharan, Professor, Rama University Uttar Pradesh, Kanpur
[2]C.S. Raghuvanshi, Professor, Rama University Uttar Pradesh, Kanpur
[3]Md. Iqbal, Professor, Meerut Institute of Engineering and Technology, Meerut

drsharan.hariom@gmail.com

Abstract:

Smart cities are rapidly developing. Currently, the successful operation of many cities throughout the world depends on a vast network of sensors, technology, and connected data-gathering portals. The use of connected technologies will increase dramatically in the future. To enhance the quality of life for their citizens, more local governments are embracing smart city technologies. This contemporary technology can offer quickly adopted answers to a wide range of issues. For instance, this new infrastructure can aid in enhancing energy efficiency, streamlining waste collection, and improving traffic flow. Cyber attacks can target smart cities in a variety of ways. Some of the most dangerous threats are advanced persistent threats (APTs). These dangers rely on a number of coordinated operations, frequently utilizing malware and "zero-day" software vulnerabilities, to interfere with urban services. However, using any technology brings up fresh problems and difficulties. A single careless act by a person or group can endanger the entire city in a "smart city." The behavior of smart cities is impacted by information-security issues (such as information leakage and harmful cyber-attacks) because so many aspects of smart cities depend on information and communication technologies. Information security must therefore advance in the same way in order to respond to the enthusiastic embrace of global smart city technology. The purpose of this article is to review pertinent literature on security in that technology as well as explain information security, smart cities, and other related topics. The current study's focus is on the four key elements of a smart city, namely the smart grid, smart buildings, smart transportation infrastructure, and smart healthcare, in order to achieve this goal.

Keywords: Information security, data protection, smart cities, smart grid, smart healthcare, software vulnerabilities

DOI Number: 10.14704/nq.2022.20.12.NQ77060 **NeuroQuantology 2022; 20(12): 769-778**

Introduction:

A technologically advanced urban setting known as a "smart city" employs various technological devices and sensors to gather certain data. In turn, the data is used to improve operations throughout the city. Information obtained from those data is used to manage assets, resources, and services effectively. To monitor and manage traffic and transportation systems, power plants, utilities, water supply networks, garbage, criminal investigations,[2] information systems, schools, libraries, hospitals, and other community services, data from residents, devices, buildings, and assets is included. [3] [4] Smart cities are those that utilize technology in innovative ways while also having effective monitoring, planning, and governing systems. [5]

The idea of a "smart city" combines information and communication technology (ICT) with

eISSN 1303-515

numerous physical devices linked to an Internet of Things (IoT) network in order to connect with inhabitants and improve the effectiveness of local operations and services. [6] [7] City officials may engage directly with both community and city infrastructure thanks to smart city technology, which also enables them to keep an eye on what is occurring in the city and how it is changing. ICT is utilized to improve urban services' quality, effectiveness, and interactivity, as well as to cut costs and resource usage and improve citizen-government interaction. [8] Applications for "smart cities" are created to control urban traffic and enable quick responses. [9] Therefore, a smart city might be more equipped to handle problems than one with a more traditional "transactional" relationship with its residents. [10] [11] Nevertheless, the phrase is still ambiguous and subject to several meanings. [12] The smart city technology has already been embraced by numerous towns.

Although creating smart cities has advantages for residents, businesses, the environment, etc., these cities are vulnerable to multiple cyber-security risks, which makes it challenging to build security maturity in them [13]. In a "smart city," one weak act by a person or group might endanger the entire community [14]. A significant difficulty for digital court investigations is this complicated city. Data and the lattice must be protected from assaults and improper behaviour in order to ensure security in a smart city [15]. The producers of the software and hardware used in smart cities rarely evaluate the cyber-security of those products. Therefore, the use of such security flaws can result in the system being hacked, being stopped, or having bogus data entered into it [16]. The preservation of privacy and citizen interactions with the government are additional issues in addition to cyber-security [17]. Users' adoption of this technology will be in doubt due to the potential for privacy invasion and the absence of cyber security in smart cities [18]. Identification of cyber security issues and privacy risks is the first step in resolving cyber security issues in smart cities and safeguarding residents' privacy [19]. One cannot successfully plan, execute, and create a smart city without being aware of these issues and offering suitable solutions [20]. On the other side, the UN estimates that by the end of 2050, there will be roughly 7.9 billion people on the planet. According to estimates, 75% of the world's population will live in cities, with some of those cities having populations of over 10 million. Deep learning is now frequently used to data that researchers have gathered. Deep learning, a sort of machine learning and artificial intelligence, has many uses in the smart city and truly mimics how the human mind learns a certain subject. Deep learning can assist the system adapt to new environments by collecting and monitoring information continually [22]. Deep learning is a subfield of artificial intelligence that enhances machine learning and neural networks. Computer vision programmes have recently significantly outperformed conventional machine learning techniques in numerous fields, including robotics, natural language processing, and many others [23]. This study aims to identify and explore the (deep learning-based) cyber security issues that smart cities face, as well as to find workable and efficient solutions to these issues or ways to lessen their effects.

Today, certain towns all around the world are embracing cutting-edge technology and becoming into "smart cities." New technologies raise the standard of living for people. Internet of Things is used to create, implement, and maintain a smart city (IoT). With the growing urbanization and proliferation of information technology, smart cities have become an emerging phenomenon. However, a smart city's

eISSN 1303-515

operation and functionality are dependent on the critical advancement of security architectures.

Cyber Vulnerabilities:

Although it's feasible to patch any exposed places, Internet of Things technology is particularly susceptible, and hackers can cause permanent harm. Large portions of the physical and digital infrastructure may need to be replaced as a result of this devastation. Here are a few of the numerous assaults that could harm the infrastructure of smart cities:

- **Asset, data, and identity theft** - Data theft is likely the most well-known cybercrime, along with asset, data, and identity theft. Data banks can be breached by hackers, who can then take personally identifying information (PII). Infrastructure in smart cities is particularly susceptible to this, and hackers have been known to steal personal information from systems supporting public payments with disastrous results.
- **Device hijacking** - One of the scarier facets of cybercrime is device hijacking. Attackers can take over a device and use it to sabotage a process by exploiting security vulnerabilities. Road signs and traffic lights are particularly at risk.
- **Man-In-The-Middle attacks** – A Man-In-The-Middle attacks occurs when a hacker may sabotage a conversation between two gadgets and pretend to be the sender, transmitting erroneous data to cause difficulties. For instance, a hacker might obtain access to a mobility platform and report delays in public transportation, which might encourage more people to drive themselves to work, resulting in an increase in traffic that paralyses a city.
- **Distributed Denial of Service** – Attacks with Distributed Denial of Service are easy. By flooding a system with requests, a hacker can disable service for those who actually need it. City systems will be unable to sustain its residents if real-life users are unable to access a service.
- **Ransom ware** – All of the aforementioned tactics might be used to kidnap a city. These are used by hackers, or activists, to compromise a process or leak private information unless particular demands are met. The practice of paying a ransom would be perilous.
- **Physical disruption** – A complicated network of connected systems can potentially be compromised via traditional physical force. Physical damage to any component could start a domino effect of destruction because many systems depend on complex procedures and feedback from networks of sensors.

These are only a few of the numerous ways malicious actors might target smart cities. The Harvard Business Review was correct when it stated that "smart cities are going to be a security nightmare." It's not all bad news, either. Cities may reduce security dangers to a minimum if the proper precautions are taken and local officials act responsibly.

eISSN 1303-515

Literature review:

The most significant of these are highlighted below. Researchers have generally examined cyber security concerns and dangers to users' privacy in smart cities from diverse points of view. Infrastructure security was identified as an important aspect in the information and data security in smart cities in a complete evaluation of research on the main security concerns and existing solutions in smart cities [24]. The advantages of urban intelligence come with several hazards and vulnerabilities in the physical-cyber substructure. Numerous security vulnerabilities exist in the primary physical-cyber systems that affect urban infrastructure, such as the delivery of electricity and water, as well as streets, buildings, etc. Cameras, communication networks, building management systems, and transportation management systems are just a few of these parts and systems. There are two categories of privacy challenges: communication and business privacy [25]. Eavesdropping, denial of service, malicious manipulation and attacks, channel attacks, detection, and secondary usage were among the difficulties to communication privacy. In addition, scams and attacks on data integrity were presenting company privacy challenges. A thorough assessment of the security of smart cities, the detection of security concerns, and in-depth knowledge of digital smart city surveys [26]. Based on civic institutions, they discovered security issues with smart grids, building automation system security, drone safety, smart vehicles, IoT sensors, and cloud storage. The functionalities of smart gadgets in linked smart buildings and their cyber security challenges [27]. They looked into some of the historical contexts surrounding the creation and need for smart device connectivity to provide users various possibilities. Then he demonstrated that despite their advantages, these technologies can pose risks and difficulties. Finally, he covered concerns about cyber-security relating to connected smart buildings and smart devices. The primary issues facing smart buildings, according to that study, were data leakage, data manipulation, data loss, and malware. The potential of already-existing smart cities around the world as well as any security issues or obstacles in their key locations [28]. He suggested that cyber security might make it possible to build a smart, secure city. In the smart city, he recognised security issues and obstacles in the areas of banking, health care, government, energy, and general security. In order to maintain cyber-security and privacy in smart cities, three solutions have been developed: manual and safe cancellation in all urban systems, access permissions, authentication, and software updates checklists for new projects, and operational plans and procedures to respond to cyber-attacks [29]. a broad analysis of the various cyber-security options using six deep learning classifiers [30]. They discussed the prospective research areas in cyber-security. a multi-view ensemble technique [31] that pooled the results of individual classifiers. A dynamic neural network technique is used in a deep learning model to forecast the performance of IoT communication systems [32]. They discovered that the strategy significantly improved sustainable smart cities and removed IoT communication system flaws. Using Hilbert-Huang transforms, fake data injection attacks in the micro-grid can be found [33]. Their research into the current and voltage signals in sensors was based on the block-chain ledger technology. They discovered that the suggested approach might boost data interchange security in the micro-grid and offer a more precise and reliable detection method.

eISSN 1303-515

Deep learning for Smart Cities:

In order to use the perceptions derived from this data to manage assets and resources, a smart city has many Internet of Things sensors at different data gathering locations to gather information on traffic, citizen mobility, and drainage [34]. DL is frequently applied to data that researchers gather. Important deep learning applications in smart cities include the ones listed below [35]:

1- Urban modeling: Several studies have utilized machine learning to pinpoint low-income neighborhoods and traffic volumes in various urban locations. Urban fashion can also be used in DL-assisted smart parking, which locates the best spot to park.
2- Infrastructure: The optimal decision may be made by applying DL on monitored data such as traffic rates, energy consumption, and other factors because infrastructure serves as the foundation of cities and plays a crucial part in resolving urban difficulties. Using ML for network routing to reduce traffic congestion is one of the applications.
3- Transportation: Through the cloud platform and AI, the transportation system links individuals, cars, supporting infrastructure, and logistics partners. In the event of accidents, one of its applications is to increase safety in transportation.
4- Urban management: Analysis of governance practices and urban characteristics, as well as understanding the evolving requirements of the smart city, are crucial functions of public management.
5- Resilience and sustainability: Over time, data creation has increased. Expanding an efficient mechanism to divide up the data that can help build smart cities is urgently needed. The scarcity of environmental resources is the biggest problem. This problem can be resolved by simulating a smart grid that reduces pollutant rates and improves quality of life. For instance, research has produced a method for using neural networks to make the best decisions on the management of industrial waste.
6- Education: The psychology of trainees can be examined through the use of big data analysis. For instance, utilizing machine learning techniques, a novel way for assessing students' engagement in classes based on their head position and facial expressions has been presented. These strategies can address the main problem with online learning, which is the lack of teacher interaction.
7- Health: Artificial intelligence has made it possible to create smart healthcare solutions using new senses like DL. Transfer learning models and DL are two ideas that have proven to be highly helpful in categorization. For instance, using these strategies has improved breast cancer diagnosis and prognosis over more conventional approaches.
8- Security and privacy: The pinnacle of outstanding ICT innovation is found in smart cities. Smart phones and artificial, integrated technologies like the Internet of Things connect city residents, enabling an unfathomable level of comfort and lifestyle improvement. These advantages are made feasible by systems like smart meters, building equipment, and health systems, but they also come with issues

eISSN 1303-515

related to data privacy and security, keeping information totality, and preventing illegal access. DL and related technologies had been successful in supplying effective IoT security breach solutions. The Random Forest method, for instance, has demonstrated success in identifying anomalies in distributed IoT devices.

The necessity for lightweight machine learning (ML) algorithms for constrained resources, datasets utilized for in-depth learning programmes that are occasionally not readily available enough to evaluate outcomes through simulation, and security-enforcing devices are challenges along the road. The camera, recording servers, and video control centre are all components of deep learning-based systems. These cameras are processed by processors like Intel and are connected to one another over a common and secure interface. The performance and power of video analysis are increased by 8–10 times by using powerful processors, and their storage space is optimized [36]. The benefit of cameras with deep learning systems is that they give warnings as soon as an illegal case is identified and red lines are formed, reducing the length of time before any action is taken, as opposed to sending all footage to the central operator. Today, the majority of cities have video systems with multiple cameras, ports, and software running at once. Hardware and software can typically communicate with one another using software development interfaces and kits, which are controlled by a single cloud management platform [37].

Prospects of Information Security in Smart Cities:

Smart Cities can reduce the risks associated with cyber security by implementing a number of safeguards and obtaining the appropriate assistance. There are two options on how to do this. The first involves paying a security firm to attempt to hack into a network and discover vulnerabilities. In essence, outside businesses will replicate assaults and look for vulnerabilities. The security firm will describe any vulnerabilities following an attack and recommend workable defenses. Although this type of penetration testing is wonderful, it is preferable to create infrastructure that is impenetrable from the start.

The second security action that cities may take is to make sure that, even in the event that hackers are successful in breaking in, their connected infrastructure remains secure. The following components must to be a regular part of a city's cyber security programme in order to keep smart cities secure:

- **Encrypted data** – There should never be a data breach. Data can be encrypted to make it useless and unreadable for everyone but those with the encryption key needed to decode it. Additionally, the encryption key should be utilized with two-factor authentication. Encryption should be utilized as normal practice because the infrastructure for smart cities deals with particularly sensitive data. In this manner, hackers won't be able to use sensitive PII data even if they get their hands on it.
- **Constant security monitoring** – A dedicated team that can monitor traffic and look for anomalies is needed for security monitoring. Security tools that can analyze large amounts of data and

eISSN 1303-515

look for signs of compromise can automate this. Potential danger areas can be isolated as soon as they are found, averting any data breaches.

- **A far-reaching support platform** – Any new platform for support should be able to secure a variety of connected environments and objects. One overarching security system needs to be implemented since smart cities are made up of many networks, SaaS, IaaS, and cloud environments. This is necessary to safeguard every component of an interconnected city.

These simple security measures can help protect a smart city.

Summary:

In this paper, information-security and data protection in the smart city were two significant and complicated topics that were looked at. There are still a lot of policies, structures, plans, and technology solutions in this crucial area as smart city cyber-security is still in its infancy. According to a study of the research literature in the area of smart cities, several studies have offered useful direction for decision-makers and city administrators who attempted to more accurately develop and implement operational plans and strategies for smart cities. A small number of studies have looked at cyber security and privacy. Other studies have defined the architecture of deploying and testing the IoT in the smart city to give a platform for testing and assessing concepts on a wide scale under real-world settings. Users in the smart city recognized that there was a clear study deficit in this field. Information theft and physical attacks that interfere with service access are both security concerns. With the increase in population information technology in cities, it is essential to have sophisticated management strategies that make use of the newest platforms and technologies to enhance urban services. A novel approach to integrating information and communication technology is seen in smart cities. Attack frequency and vulnerabilities will rise when systems are connected and integrated. On the other hand, privacy will become less secure as more information on the whereabouts and activities of digital citizens is produced. As a result, it's critical to offer solutions that emphasize long-term cyber security and risk management techniques. The findings of this study indicated that governments, manufacturers of hardware and software, and businesses offering IT security services must all work diligently to overcome these obstacles. Additionally, it is crucial to have adaptable systems with strong information protection capabilities in order to stop severe security breaches because these occurrences can result in disastrous losses in terms of money, data, credit, and public confidence. It is advised that future study develop an evaluation and grading system because risks to user privacy and cyber security are not equally important in the smart city and relevant authorities and policymakers have limited resources to address them.

Cyber Security: Best Practices:

One option to ensure the security of smart city services is to invest in pricey security measures, but there are several less expensive procedures that can foster safer interconnectivity. Here are some things to remember:

eISSN 1303-515

- **Learn everything about new technology before implementing it** – Instead of hastily implementing a novel system, give it time to be studied and any possible flaws addressed.
- **Start small** – Start with a modest proof-of-concept and check if it can withstand a simulated cyber attack before installing a larger system. It is not ready for city-wide implementation if it doesn't hold up.
- **Create a dedicated security team** – Employ IT experts with security experience. The right team will be able to conduct penetration tests, evaluate vulnerabilities, and provide fail-safe and override tools.
- **Avoid over-reliance on smart technology** – It's simple to get caught up in relying only on one method of doing things.
- **Always prepare for the worst** – The prepared person gets lucky. Always plan for the worst-case scenario to make sure you're prepared in the event that your city is the target of a cyber attack.

In conclusion, a smart city is only as smart as those who run it. You're safeguarding yourself and your fellow people when you safeguard a city's smart systems. We should all be a little more serious about information security.

References:

1. *Goldsmith, Stephen (16 September 2021). "As the Chorus of Dumb City Advocates Increases, How Do We Define the Truly Smart City?". datasmart.ash.harvard.edu. Retrieved 27 August 2022.*
2. *Fourtané, Susan (16 November 2018). "Connected Vehicles in Smart Cities: The Future of Transportation". Interesting Engineering.com. Retrieved 27 August 2022.*
3. *McLaren, Duncan; Agyeman, Julian (2015). Sharing Cities: A Case for Truly Smart and Sustainable Cities. MIT Press. ISBN 9780262029728.*
4. Jump up to:[a] [b] *Musa, Sam (March 2018). "Smart Cities-A Road Map for Development". IEEE Potentials. **37** (2): 19–23. doi:10.1109/MPOT.2016.2566099. ISSN 1558-1772. S2CID 3767125. Retrieved 27 August 2022.*
5. *Mills, David; Pudney, Steven; Pevcin, Primož; Dvorak, Jaroslav (January 2022). "Evidence-Based Public Policy Decision-Making in Smart Cities: Does Extant Theory Support Achievement of City Sustainability Objectives?". Sustainability. **14** (1): 3. doi:10.3390/su14010003. ISSN 2071-1050.*
6. *"The 3 Generations of Smart Cities". 10 August 2015. Archived from the original on 9 October 2017. Retrieved 17 October 2017.*
7. *Peris-Ortiz, Marta; Bennett, Dag R.; Yábar, Diana Pérez-Bustamante (2016). Sustainable Smart Cities: Creating Spaces for Technological, Social and Business Development. Springer. ISBN 9783319408958. Archived from the original on 30 October 2020. Retrieved 4 October 2020.*
8. *"Building a Smart City, Equitable City – NYC Forward". Archived from the original on 4 December 2017. Retrieved 4 December 2015.*
9. Jump up to:[a] [b] [c] [d] [e] *Komninos, Nicos (22 August 2013). "What makes cities*

eISSN 1303-515

intelligent?". In Deakin, Mark (ed.). Smart Cities: Governing, Modelling and Analysing the Transition. Taylor and Francis. p. 77. ISBN 978-1135124144.

10. Department for Business, Innovation and Skills (2013), p. 7 "As consumers of private goods and services we have been empowered by the Web and, as citizens, we expect the same quality from our public services. In turn, public authorities are seeking to reduce costs and raise performance by adopting similar approaches in the delivery of public services. However, the concept of a Smart City goes way beyond the transactional relationships between citizen and service provider. It is essentially enabling and encouraging the citizen to become a more active and participative member of the community"
11. *Chan, Karin (3 April 2017). "What Is A 'Smart City'?". Expatriate Lifestyle. Archived from the original on 24 January 2018. Retrieved 23 January 2018.*
12. *Hunt, Dexter; Rogers, Christopher; Cavada, Marianna (2014). "Smart Cities: Contradicting Definitions and Unclear Measures". MDPI Sciforum – The platform for open scholarly exchange. sciforum.net. pp. f004. doi:10.3390/wsf-4-f004. Archived from the original on 22 March 2016. Retrieved 16 March 2016.*
13. Baig, Z.A., et al., 2017. Future challenges for smart cities: Cyber-security and digital forensics. Digit. Investig. 22, 3–13
14. Zhou, X., et al., 2021. Information diffusion across cyber–physical-social systems in smart city: A survey. Neurocomputing 444, 203–213.
15. Sengan, S., et al., 2020. Enhancing cyber–physical systems with hybrid smart city cyber security architecture for secure public data-smart network. Future Gener. Comput. Syst. 112, 724–737.
16. Sengan, S., et al., 2021. Detection of false data cyber-attacks for the assessment of security in smart grid using deep learning. Comput. Electr. Eng. 93, 107211.
17. Chen, D., Wawrzynski, P., Lv, Z., 2021. Cyber security in smart cities: A review of deep learning-based applications and case studies. Sustainable Cities Soc. 66, 102655.
18. Lim, C., Cho, G.-H., Kim, J., 2021. Understanding the linkages of smart-city technologies and applications: Key lessons from a text mining approach and a call for future research. Technol. Forecast. Soc. Change 170, 120893.
19. El Hilali, S., Azougagh, A., 2021. A netnographic research on citizen's perception of a future smart city. Cities 115, 103233.
20. Kashef, M., Visvizi, A., Troisi, O., 2021. Smart city as a smart service system: Human–computer interaction and smart city surveillance systems. Comput. Hum. Behav. 124, 106923.
21. Atitallah, S.B., et al., 2020. Leveraging deep learning and IoT big data analytics to support the smart cities development: Review and future directions. Comp. Sci. Rev. 38, 100303.
22. Singh, S.K., Jeong, Y.-S., Park, J.H., 2020. A deep learning-based IoT-oriented infrastructure for secure smart city. Sustainable Cities Soc. 60, 102252

23. Belhadi, A., et al., 2021. Deep learning for pedestrian collective behavior analysis in smart cities: A model of group trajectory outlier detection. Inf. Fusion 65, 13–20.
24. AlDairi, A., 2017. Cyber security attacks on smart cities and associated mobile technologies. Procedia Comput. Sci. 109, 1086–1091.
25. Ijaz, S., et al., 2016. Smart cities: A survey on security concerns. Int. J. Adv. Comput. Sci. Appl. 7 (2), 612–625.
26. Baig, Z.A., et al., 2017. Future challenges for smart cities: Cyber-security and digital forensics. Digit. Investig. 22, 3–13
27. Arabo, A., 2015. Cyber security challenges within the connected home ecosystem futures. Procedia Comput. Sci. 61, 227–232
28. Thing, V.L., 2014. Cyber security for a smart nation. In: 2014 IEEE International Conference on Computational Intelligence and Computing Research. IEEE.
29. Alibasic, A., et al., 2016. Cybersecurity for smart cities: A brief review. In: International Workshop on Data Analytics for Renewable Energy Integration. Springer.
30. Chen, D., Wawrzynski, P., Lv, Z., 2021. Cyber security in smart cities: A review of deep learning-based applications and case studies. Sustainable Cities Soc. 66, 102655.
31. Fard, S.M.H., et al., 2020. Ensemble sparse representation-based cyber threat hunting for security of smart cities. Comput. Electr. Eng. 88, 106825.
32. Said, O., Tolba, A., 2021. Accurate performance prediction of IoT communication systems for smart cities: An efficient deep learning based solution. Sustainable Cities Soc. 69, 102830
33. Ghiasi, M., et al., 2021a. Cyber-attack detection and cyber-security enhancement in smart DC-microgrid based on blockchain technology and Hilbert Huang transform. IEEE Access 9, 29429–29440.
34. Basori, A.H., et al., 2019. iMars: Intelligent municipality augmented reality service for efficient information dissemination based on deep learning algorithm in smart city of Jeddah. Procedia Comput. Sci. 163, 93–108
35. Li, D., et al., 2019. IoT data feature extraction and intrusion detection system for smart cities based on deep migration learning. Int. J. Inf. Manage. 49, 533–545.
36. Ahmed Jamal, A., et al., 2021. A review on security analysis of cyber physical systems using machine learning. Mater. Today: Proc.
37. Sahil, Sood, S.K., 2021. Smart vehicular traffic management: An edge cloud centric IoT based framework. Internet of Things 14, 100140.