Computing and Informatics, Vol. 41, 2022, 405–423, doi: 10.31577/cai_2022_2_405

SMART CITIES SECURITY THREAT LANDSCAPE: A REVIEW

Raja Waseem Anwar

Arab Open University
Muscat, Sultanate of Oman
e-mail: waseem@aou.edu.om

Saqib Ali

Sultan Qaboos University
Muscat, Sultanate of Oman
e-mail: Saqib@squ.edu.om

Abstract. There has been a swift rise in the development of smart cities. This evolution has been prompted by the rise in emerging technologies such as edge computing, IoT, data science, and analytics. Combining these technologies has paved the way for new, automated systems for managing and monitoring procedures and industries, resulting in increased efficiency and improved quality of life. While these interconnected services assist in managing the growing population in the urban environments through efficient service delivery and increased operational efficiency, they also increase the risk of adversary threats, security, and privacy challenges to smart cities. This paper presents the holistic view of the security landscape and highlights the security threats, challenges, and risks to the smart city environment.

Keywords: Smart cities, IoT, data science, security, threats, privacy, risk

1 INTRODUCTION

In the last few decades, provisioning smart cities have become the prime focus due to facilities offered such as economic development, improved infrastructure,

and efficient data-driven decision making capabilities. According to the predictions by the United Nations (UN, 2014), 50 % of the global population will live in cities by 2050. However, the increase in urbanization imposes several challenges, such as environmental pollution, traffic congestion, governance, financial issues, infrastructure limitations, and the availability of clean water [1, 2]. To overcome these challenges and improve the quality of services, it is required to build fundamental infrastructure and enhance service delivery, manage everyday operations with access to basic urban facilities like affordable housing, education, and quality healthcare services. Smart cities are focusing on improving people's lives by reforming infrastructures and services. At present, various countries are moving in this direction and adopting information and communication technologies to develop smart cities like in China where around two hundred smart city projects are in progress [3, 4].

Internet of Thing (IoT) is the key enabling technology for smart cities and provides all the essential building components such as sensors, actuators, and other communication technologies that are required to perform operations like smart meters for parking, controlling the street lights, smart health monitoring, traffic monitoring, and optimizing routes to provide a comfortable life to residents [5]. The applications in smart cities utilize cloud-based centralized data storage. Moreover, the integration of sensing components performs real-time monitoring and communicates back to the physical world for decision making. However, this constant growth and increase in rapid urbanization have led to challenges for traditional safety and security in smart cities due to complex and inherent integration with IoT [6]. In addition, smart cities are prone to a diverse set of cybersecurity threats and attacks due to heterogeneity (complex systems), scalability, dynamic characteristics, and a higher degree of interdependence between components, for instance, if the sensing services get disrupted due to exploitation of vulnerabilities or inclusion of malicious nodes, the adversaries can manipulate the sensed data that can negatively impact the decision making capabilities resulting in degradation of the quality of services. Therefore, providing security and protecting the privacy of these devices is a real challenge that must be addressed [7].

Security concerns related to smart cities vary from application environment to networking and communication technologies. Without gauging sufficient security and privacy, citizens may feel hesitant in residing in the smart city [8]. Besides, the inherent characteristics and advantages of using wireless sensor networks (WSNs), Internet of Things (IoT), Cloud, Edge, and Next-Generation Networks (NGN), increases the security threats to smart cities. Securing smart cities from adversaries and cyberattacks is equally critical and challenging. Since the threat landscape is changing rapidly and exploiting the vulnerabilities may put the smart cities' resources and services in danger.

There are several traditional security measures available such as encryption and biometric authentication, but these measures are less effective in securing Smart cities due to limited computational capabilities for deploying various sensors. Furthermore, the advancement in information technologies such as artificial intelligence,

machine learning, and data mining has increased the chances of attacks where adversaries using advanced technologies can easily bypass the traditional security techniques. Preserving users' privacy in a smart city is another equally important issue to consider while proposing the security solution [9]. Security issues are not new, however, the advances in technology make it necessary to produce new and innovative ways to protect data and privacy [10].

This paper highlights the vulnerabilities with associated attacks for the smart cities and presents the open issues such as up-to-date requirements for security and challenges which could build the foundation for developing more secure and privacy-protected futuristic smart cities.

The sections of the paper are organized as follows. Section 2 discusses the related work comprising relevant studies focusing on security risks and threats associated with smart city's environment. Section 3 presents the IoT architecture for smart cities. Sections 4 and 5 discuss the elements of a smart city and its architecture. Sections 6 and 7 highlight the security measures, threats, attacks related to smart cities. Lastly, the Sections 8 and 9 present the direction for future work and the conclusion.

2 RELATED WORK

The technological advancement has resulted in a significant rise in the adoption of smart devices and ecosystems for automating industries like transportation, healthcare, education, and logistics. The realms of data science, big data analytics, and IoT play a vital role in the planning and development of smart cities [11]. The idea behind smart cities is to utilize these edge-cutting technologies for transforming regular cities into intelligent cities comprising end-to-end automation of conventional processes [12]. According to [13, 14], smart cities encompass numerous IoT devices. These widely interconnected services generate tons of structured, unstructured, and semi-structured data. Given the inevitable data collection through IoT devices, one of the prominent technical issues in the smart city ecosystem is unstructured data management [12]. All the collected data is not beneficial unless it is cleaned and modeled for insights and analysis. This is where data science plays a crucial role in modeling the data for generating valuable insights that can assist in the successful implementation of smart city structure in alliance with the technological infrastructure [15]. In addition to technological challenges, other challenges can also be tackled through the implications of data science. The collection, aggregation, and analysis of the real-time data can help the government in making informed decisions, devising effective waste reduction methodologies, and many more smart capabilities [15]. Overall, the implementation of data science technologies in conjunction with IoT for smart cities infrastructure can provide information for effectively managing the resources for enhancing the quality of life for the smart cities' residents.

Numerous researchers have discussed the role of technology and proposed frameworks for designing the structure of smart cities. The paper [16] presents the framework for understanding the core components of smart cities in terms of the key factors driving the initiative of smart cities namely people, environment, governance, technology, policy context, and economy. In addition to the key drivers of smart cities, the authors have also discussed the core challenges in three domains namely, IT infrastructure, security and privacy, and operational cost. Overall, the paper defines the important aspects of the smart cities' initiative however, the paper has not discussed the ideal technologies that can be used for designing the smart cities' infrastructure. This limitation has been covered in the paper [17] where the authors have discussed the importance of IoT, data science and analytics, and related data sources generating real-time data for analyzing and monitoring smart infrastructures such as smart transportation, resource efficiency, crowd source-based services. However, it does not comprise the risks and threats associated with the smart cities' architecture. In comparison to the previously defined papers, the proposed paper demonstrates a systematic view of the security requirements, threats, and attacks associated with the smart cities' infrastructures.

3 GENERIC IOT ARCHITECTURE FOR SMART CITIES

In general, Internet of Things (IoT) is defined as decentralized systems of smart objects having sensing and processing capabilities with the ability to communicate with other network components [18]. Moreover, due to the diverse range of devices, underlying technology, and integration of components, it is difficult to define a general architecture for smart cities. However, the basic communication frame for a smart city consists of three layers, i.e., perception or hardware layer, network layer, and application layer. These layers work together and establish communication among various entities and other network components [19]. Each layer in the architecture is responsible for collecting, processing, and analyzing the data. For instance, the perception layer, also known as the recognition layer, is the lowest in the architecture. It perceives the environment, collects real-time data, and forwards the acquired information to the network layer for further processing. The devices at this layer are RFID and smart sensors which monitor almost anything in the city landscape, for instance monitoring the environmental factors such as brightness, sound, and even participatory sensing through social media [19]. The sensors deployed at the perception layer play a crucial role in generating real-time data with the cooperation of other nodes in local network domains that are then aggregated and analyzed at the application layer [21]. The second layer – the network layer, also known as the transmission layer, is the core layer in IoT architecture that connects the perception layer with the application layer. The main responsibility of the network layer is to provide long, and short-range communication and routing using sensors, servers, storage devices and perform the aggregation of data from other sensors [22]. Also, the important contributor to communication at this

layer are the Wireless Sensor Networks (WSNs) routing protocols for the devices to communicate with each other and with the gateway. Similarly, cloud computing, Wi-Fi, LTE, Bluetooth, ZigBee, 4G/5G are also a part of this layer. The topmost layer is the application layer that is responsible for providing services to various applications such as smart city, smart grid, and smart health. Also, this layer handles the decision making process and controls commands to efficiently handle the aggregated data [23]. Figure 1 depicts the IoT-based layered architecture for smart cities.

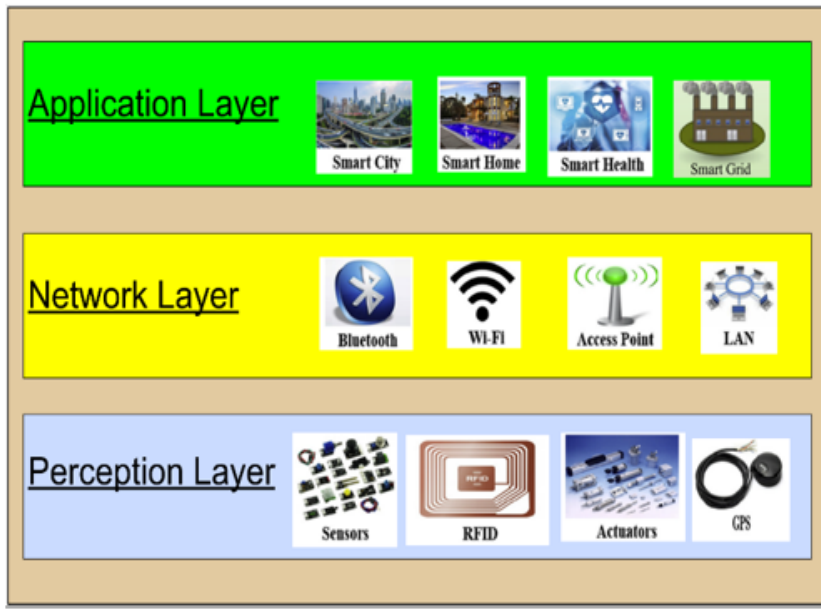

Figure 1. Generic IoT layered architecture for smart cities

The distinction between these layers helps to understand the complexity and heterogeneity of devices and communication patterns employed in smart cities. Moreover, smart cities are becoming smarter due to the enriching nature of digital technologies deployed and hailed as the modern way forward for any urban area.

4 KEY ELEMENTS OF SMART CITY

Smart city elements positively impacted people's lives due to the offered benefits and quality of services provided. According to the National Institute of Standards and Technology (NIST), one of the most widely and adopted reference models for smart cities categorizes six distinctive areas as smart people, smart economy, smart

governance, smart environment, smart mobility, and living [2, 22]. However, there are various priorities and constitutions of smart cities from one location to another, for example, design and deployment of wastewater management have a higher priority at one place while on the other location it is disaster management [23]. Some of the key elements of smart cities are as follows.

4.1 Smart Living

Smart living aspires to provide basic services to its citizens by providing smart buildings, smart homes, and the inclusion of fundamental infrastructure and architectural components that must be in place to make the city smart. Moreover, smart living provides a secure environment that ensures the safety and security of all citizens. Providing a healthy atmosphere will have a positive impact on people's lives which will not only actively influence the behavior of people but also increase their creativity [24].

4.2 Smart Mobility

Mass transit and other types of public transportation are the main elements in smart cities where many people are commuting. Like other smart applications, Intelligent Transportation Systems (ITS) are equipped with embedded sensors, communication, and navigation systems where all the vehicles are connected. Similarly, various other types of IoT sensors are deployed and maintained to monitor the environment, gather the data, and respond to changes in the smart city environment [25]. In addition to this, they can also secure road transport, railway, and marine services by establishing online schedules and real-time tracking. Lastly, the use of electric vehicles reduces carbon emissions and provides a pollution-free environment.

4.3 Smart People

To get the maximum benefits, people living in smart cities need to be aware of various aspects such as protection of the environment, sustainable adoption of a healthy lifestyle, recycling, and saving water and energy [24]. In addition, the use of technology facilitates the inclusion of people to involve in discussions with the government, other key stakeholders, and ultimately in the decision making process.

4.4 Smart Economy

Smart economy refers to promoting local growth by enhancing the digital economy, paving way for entrepreneurship, and a flexible labor market. Implementing a smart economy would add value to the smart city where diverse and flexible opportunities will become available for the citizens. Moreover, the innovation and entrepreneurship activities can foster a positive and competitive business environment that could

promote growth for smart cities. In addition to this, economic growth has a positive impact on people's lives as it promotes forward-thinking and could help in reaching global businesses [26].

4.5 Smart Environment

In the development and progression of a sustainable society, smart environment plays a substantial role in the management of smart buildings, traffic congestion, waste control systems, and in monitoring air pollution using ubiquitous sensing, for example, the utilization of waste to produce environment-friendly fuel and energy, the treatment of wastewater, and recycling of waste. In addition, the smart environment ensures the optimal usage of resources and improving performance through various software and hardware devices [27].

4.6 Smart Governance

Management of smart city governance is very crucial since it requires overseeing day-to-day operations, serving citizens, and the community at large. Also, smart governance allows the citizens to participate in the decision making process which not only helps in better city planning and development but giving an equal opportunity to all [42]. Figure 2 summarizes the various elements of smart cities.

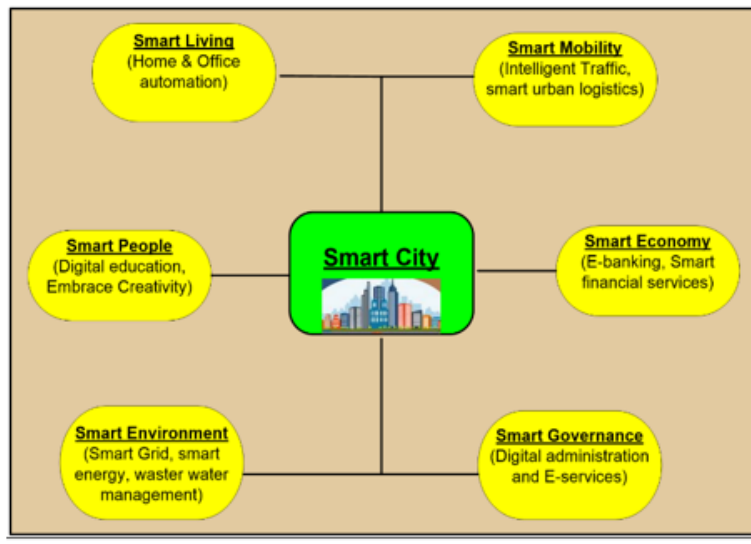

Figure 2. Key elements of smart city

5 SMART CITY ARCHITECTURE

Since the inception of the smart city paradigm, various ICT architectures have been proposed based on different security requirements and characteristics. Moreover, there is no unique standardized architecture and common security framework for a smart city which is a major problem. However, ubiquitous sensing allows collection of information from the physical world (sensing), processing it, and decision making through a communication world using heterogeneous network components, processing units, and control operating components. In addition, smart city architectures are differentiated according to the characteristics of perception, network, and application layers where each layer provides services (service-oriented architecture) and works with other layers in a collaborative manner. However, the following characteristics of smart cities must be considered before developing any security and privacy protection mechanism [28, 29].

5.1 Heterogeneity

The heterogeneity of various sensing devices and networks plays an instrumental role in supporting the smart city infrastructure. However, the dynamic nature and the diversity of devices, components, protocols, and architectures within the smart city are often incompatible. Also, during the implementation, the interoperability issues might cause systems to malfunction which impacts the performance gain [29]. In addition, the connectivity between Wireless Sensor and Local Area Networks (WLANs) with other devices and cellular networks requires seamless integration.

5.2 Sensing Components

To bridge the gap between sensing (physical world) and communication, there are various types of sensors such as temperature sensors, industrial sensors, smart metering sensors, and video surveillance devices that can be deployed to sense the phenomenon and gather the information which is then processed further for decision making. However, the major issue with these sensors is limited energy, computational power, memory, and processing capabilities [29].

5.3 Resource Constraint

Considering the vital role of energy storage, smart cities face the resource constraint challenge due to the inherent characteristics of IoT and the wide-scale deployment of embedded sensors. Also, these sensors are battery-operated with limited storage and processing capabilities. In addition, the inclusion of a malevolent node quickly depletes the battery energy [30].

5.4 Scalability

Smart Cities are growing at a rapid pace hence more data and network traffic are generated. Also, the addition of new components and services to an existing network requires scalability and resilience. Therefore, it is equally important to consider the scalability issue in the design of smart cities.

5.5 User Involvement

System users are the main stakeholders in smart cities since they are directly benefitting from the services. Moreover, the user's involvement in the system not only increases the performance but also enhances the decision making process [30].

6 SECURITY MEASURES FOR SMART CITY

Cities are becoming smarter hence provisioning the required security and privacy in a smart city environment is equally important and challenging. Like any other network and system, providing security to smart city services/entities requires special considerations due to the heterogeneity of devices, the multitude of communication protocols, the interconnectivity of various components, and insufficient computational capabilities. In addition, without a proper security solution, the inclusion of sensor nodes is often prone to internal and external attacks. Moreover, smart city applications use wireless sensor networks where the interaction between cyber and physical components for gathering and processing the data makes an ideal target for adversaries [31]. In an unprotected environment, mutual authentication is required for the communication process to ensure the security of smart city applications.

A growing concern for smart cities is cybersecurity which is considered the most vital issue [32]. Any security breach can cause catastrophic effects such as financial and information loss, and physical harm due to the insertion of incorrect data into the system resulting in a disruption in the various operations in smart cities. The main objective of security in smart cities is to protect physical assets, data, and networks from known and unknown vulnerabilities, threats, and attacks. In addition, the diverse range of devices generates a massive amount of data that is used in the decision making process. Moreover, this collected data is considered the most critical asset and requires proper security for protecting its confidentiality, integrity, availability (CIA), authenticity, and validation. Integrity is the trust in the truthfulness of the resources in the systems that ensure that the performed operations are carried out by the intended and authorized user [33]. Thus, smart cities need to maintain their data integrity and implement the necessary precautionary measures to repel the attack from adversaries and from eavesdropping the communication. Similarly, it is also mandatory to maintain the confidentiality of data and communication among systems and ensure the complete security of the smart cities

by achieving a sense of availability, authenticity, validation for data and transactions [34]. Devices that work at various layers of IoT based smart cities are prone to failure due to resource constraint and vulnerabilities that are prone to threats and attacks, for instance, sensors, cameras, and actuators are collecting and sharing sensitive data which could be intercepted by malicious adversaries hence threatening the security and privacy of user data in smart cities [35]. Table 1 summarizes the various security requirements which must be considered during the design and authentication stage among different components of smart cities.

Security Requirements for Smart Cities	**Description**
Confidentiality	The protection of data between communication entities from unauthorized access.
Integrity	Ensuring the security of data from alteration or modification from a malicious user while the data is fetched through sensors and transferred to centralized authority such as base station (BS) or communication center.
Availability	The continued availability of devices and services of smart city entities whenever required by the user.
Authentication	Identification of communicating peers.
Authorization	Only authorized parties have access to available resources and services.
Non-repudiation	Communicating parties cannot deny the transactions made among them.
Data Freshness	Enabling the assurance of data generated by smart city devices are fresh with time-stamped and no adversary has altered the data or replays the old messages.
Anonymity	Ensuring the information is protected and inaccessible to an adversary.
Scalability	The ability of the system to provide services successively while adding the new devices and services to an existing system.
Attack Resistance	Resiliency against various potential attacks.

Table 1. Security requirements for smart cities

6.1 Distinguishing Characteristics of Smart City Security

Smart cities are facing the large number of security challenges which range from technical problems to complex attacks due to distinguishing characteristics, therefore, the smart city requires special security consideration as compared to traditional IT systems and networks where proposed techniques and countermeasures are devel-oped based on conventional network security. Also, protecting the smart city compo-nents is challenging due to the heterogeneity of devices, insecure and

hostile envi-ronments, and inadequate protection of data and privacy, for example during data transmissions, protection of devices, and security of data storage devices [28, 29]. The following subsections describe these requirements.

6.2 Protection of Devices

Normally, the protection mechanism for smart devices is based on cryptography, which is often infeasible due to the limited processing capabilities of sensors and actuators. Moreover, authentication is considered as the first line of defense against unauthorized access. If an authentication mechanism is weak then adversaries can access resources and manipulate the system and data [28].

6.3 Secure Data Transmission

The massive increase in data exchange among multiple services and assets requires proper security controls to protects the integrity of data and to detect malicious activities. In addition, secure data transmission reduces the impact of data theft and misuse including denial of service (DoS) attacks where the malicious attackers could capture the transmission and manipulate the messages [30].

6.4 Securing Applications

Ubiquitous and embedded computing is constantly increasing in the consumer domain where a diverse set of smart devices and applications are interacting with each other hence turning them into attack vectors. Moreover, most of the smart city applications leverage the same architecture and even face similar vulnerabilities. Therefore, proposing a single security solution could be implemented across applications [31].

7 SECURITY THREATS AND ATTACKS TO SMART CITY

Security refers to a state of being safe and protected. With references to smart cities, security includes precautionary measures essential for protecting the city and its citizens from direct or indirect harm resulting from unlawful access to information and cyber or physical attacks that can disrupt the system [36].

Unlike traditional security mechanisms, smart city security requires new and innovative ways of securing the devices and applications while considering the characteristics such as resource constraints, distributed architecture nature, and geographic distribution. Smart cities are prone to several unique challenges such as unreliable communication, inadequate level of data, and privilege protection.

Providing the required services round the clock uninterruptable is the main objective of smart cities. Also, the unavailability of any service could have a catastrophic impact. However, smart cities are exposed to several attacks due to the

integration of various technologies, software, hardware that is prone to incompatibility hence the attacker can exploit these vulnerabilities that could cause server damage to the physical environment [27, 37]. Another aspect of vulnerability is the distributed nature of smart city networks where numerous tiny sensors and other resource constraint devices are incorporated together that is an ideal target for attackers. Therefore, smart cities need to ensure the complete end-to-end security of the system by placing the necessary controls and countermeasures. The layered architecture (Figure 1) plays a vital role in developing smart cities' security since each layer involves communication and is susceptible to either internal, external, or internet attacks.

It is challenging to adopt a unified and consolidated security mechanism for smart cities because of the dynamic environment, internet connectivity, and layered architecture. Therefore, an effective security mechanism that preserves privacy and security must be included in all participating layers. A brief description of attacks that occurs at various layers of smart cities is described in the following subsections.

7.1 S Attacks at the Perception Layer

The devices that work at the perception layer are sensors, tags, RFID, actuators, and GPS, which have limited energy, computational power, and memory. Moreover, the placement of these devices is usually in open and hostile environments where adversaries can capture them physically, tamper, or even get the keys. Therefore, these devices are susceptible to a variety of attacks [38]. Thus, it is important to protect the devices and put the necessary measures in place to prevent information disclosure and to reduce the attack impact. The common attacks at the perception layer are [34, 39]:

Denial of Service (DoS) attack: In this attack, network services are unavailable to legitimate users because all the available resources are flooded with false messages and fake requests that make the network inaccessible.

Eavesdropping: The attacker monitors the network to obtain sensitive information that they later use for launching the attack.

Man-in-the-Middle (MITM): Adversary controls the communication channel through obtaining control between two systems.

Malicious node: The inclusion of malicious nodes in the existing network not only spreads false information but threatens the network's security, data integrity, and availability.

Resonance attack: During resonance attacks, the forged sensor which uses different frequencies disrupts the communication among legitimate components.

7.2 Attacks at the Network Layer

The network layer is responsible for the transmission and routing of data. However, due to the nature of communication, this layer could face radio interference, data leakage, and interruption problems. Moreover, several security attacks can threaten the network layer and the availability of services. The common attacks which occur at this layer are [10, 40]:

Jamming attack: The jamming attack is one of the most common attacks especially for sensor-based networks where the communication is corrupted by jamming signals which result in damaging the ongoing communication between devices and eventually reduces the bandwidth availability.

Routing attack: Inclusion of malicious nodes to the network creates forge paths and routing loops which increase the transmission delay and overhead.

Selective-forwarding attack: In this attack, the compromised node drops some of the legitimate data packets and forwards a few selected packets.

Sleep deprivation attack: During a sleep deprivation attack, the intruder constantly sends the messages to the sensor node to drain its energy so the life-time of the network is minimized.

Wormhole attacks: Constituting the communication network multiple malicious nodes participate in this attack and create the information hole in the network through the creation of false routes.

Sinkhole attack: In the sinkhole attack, the compromised node propagates the forge path information to other nodes to re-route the traffic. Also, this attack is used to launch other similar attacks.

7.3 Attacks at the Application Layer

One of the most important layers in smart city architecture is responsible for exchanging a large amount of user data among various entities and applications. The application layer faces most threats related to user data, privacy, and unauthorized access to resources. Also, the application layer can be configured in different ways according to the level of services provided. The common attacks at this layer include [35, 41]:

Buffer overflow: Software vulnerabilities are exploited through buffer over-flow and then attacks are launched.

Malware attack: The attacker deploys the malicious software to gain unauthorized access to the network and resources by exploiting the vulnerabilities.

Social engineering attacks: In this attack, the adversary captures and manipulates people's personal information such as pin number and password through email or website.

SQL injection attack: An input string is injected into the database through the application which changes the SQL statements and the attacker gains control over the database and gets access to information.

Providing appropriate security at each layer is challenging due to interaction and dependency among the layers and components. Moreover, the vulnerabilities which are exploited by adversaries cause damage to services. Therefore, the provision of robust security needs to be in place that can prevent, detect, and mitigate possible attacks. Table 2 summarizes the various security attacks, their countermeasures that occur at different layers of smart cities that should be considered while designing the security solutions.

Layer	Elements	Security Threats	Attacks	Security Parameters	Countermeasures
Perception Layer	• Sensors • RFID • Actuators • GPS	• Physical Capture • Malicious node • Privacy	• Denial of Service (DoS) • Eavesdropping • Man-in-the-Middle (MITM) • Malicious node • Resonance	• Confidentiality • Authentication • Integrity • Trust Mechanism	• Encryption • Access Control • Trust Management • Secure Routing
Network Layer	• Bluetooth • Wi-Fi • Access Points (Aps) • LAN	• Communication Disruption • Denial of Service (DoS) • Network Routing	• Jamming • Routing • Selective forwarding • Sleep deprivation • Wormhole • Sinkhole	• Confidentiality • Authentication • Integrity • Trust Mechanism • Confidentiality • Integrity • Availability • Authentication	• Access Control • Authentication • Secure Routing • Attack Detection
Application Layer	• Smart Home • Smart Health • Smart Grid	• Privacy • Information Interception • Access Control • Denial of Service (DoS)	• Malware attack • Buffer overflows • Social Engineering • SQL Injection attack	• Authentication • Availability • Privacy • Integrity • Non-repudiation	• Authentication • Authorization • Encryption • Trust Management • End-to-End encryption

Table 2. Summary of smart city security attacks

8 OPEN ISSUES, CHALLENGES AND FUTURE RESEARCH

Directions for the significant growth and the provision of services provided by smart cities to its resident are phenomenal. However, the interdependency between the various components/objects of smart cities possesses significant threats and security challenges that need to be addressed at the early stages. Some of the future research directions and challenges are:

- Since smart cities are interdependent and rely on critical infrastructures, therefore, changes in one major process can slow down or disrupt services in mission-critical industries such as the healthcare and telecommunication industries.
- The resource-constraint devices such as sensors that play an important role in sensing and acquiring the information are vulnerable to both internal and external attacks, therefore, they can be easily disrupted or penetrated via the denial-of-service or man-in-the-middle attacks.

From the above analysis, it can be concluded that the diverse and complex environment of smart cities requires proper standardization of security measures with new and vibrant frameworks that ensure end-to-end security between the layers and among the resource-constraint devices.

9 CONCLUSION

Smart cities are emerging and comprise a plethora of interconnected devices, therefore, the provision of security and privacy is challenging. This paper highlights a brief review of security threats and challenges faced by smart cities and their applications. The interconnectivity and the complex heterogeneity between the physical and cyberinfrastructure of smart cities require special security countermeasures. The architecture of smart cities is discussed followed by the various attacks at Network, Perception, and Application layers. Overall, this review paper serves as a valuable resource and reference point for academia and industrial practitioners.

REFERENCES

[1] DeLuca, L.: United Nations: Online Data Repositories and Resources. College and Research Libraries News, Vol. 78, 2017, No. 1, pp. 41–45, doi: 10.5860/crln.78.1.9607.

[2] Khatoun, R.—Zeadally, S.: Smart Cities: Concepts, Architectures, Research Opportunities. Communications of the ACM, Vol. 59, 2016, No. 8, pp. 46–57, doi: 10.1145/2858789.

[3] Yang, Y.—Wang, X.—Zhu, S.—Cao, G.: Distributed Software-Based Attestation for Node Compromise Detection in Sensor Networks. 2007 26th IEEE International Symposium on Reliable Distributed Systems (SRDS 2007), 2007, pp. 219–230, doi: 10.1109/SRDS.2007.31.

[4] Zhang, K.—Ni, J.—Yang, K.—Liang, X.—Ren, J.—Shen, X. S.: Security and Privacy in Smart City Applications: Challenges and Solutions. IEEE Communications Magazine, Vol. 55, 2017, No. 1, pp. 122–129, doi: 10.1109/MCOM.2017.1600267CM.

[5] Hammi, M. T.—Hammi, B.—Bellot, P.—Serhrouchni, A.: Bubbles of Trust: A Decentralized Blockchain-Based Authentication System for IoT. Computers and Security, Vol. 78, 2018, pp. 126–142, doi: 10.1016/j.cose.2018.06.004.

[6] Gamundani, A. M.: An Impact Review on Internet of Things Attacks. 2015 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC), 2015, IEEE, pp. 114–118, doi: 10.1109/ETNCC.2015.7184819.

[7] Mao, Y.—You, C.—Zhang, J.—Huang, K.—Letaief, K. B.: A Survey on Mobile Edge Computing: The Communication Perspective. IEEE Communications Surveys and Tutorials, Vol. 19, 2017, No. 4, pp. 2322–2358, doi: 10.1109/COMST.2017.2745201.

[8] Anwar, R. W.—Zainal, A.—Outay, F.—Yasar, A.—Iqbal, S.: BTEM: Belief Based Trust Evaluation Mechanism for Wireless Sensor Networks. Future Generation Computer Systems, Vol. 96, 2019, pp. 605–616, doi: 10.1016/j.future.2019.02.004.

[9] Butt, T. A.—Afzaal, M.: Security and Privacy in Smart Cities: Issues and Current Solutions. In: Al-Masri, A., Curran, K. (Eds.): Smart Technologies and Innovation for a Sustainable Future, Springer, Cham, Advances in Science, Technology & Innovation (IEREK Interdisciplinary Series for Sustainable Development), 2019, pp. 317–323, doi: 10.1007/978-3-030-01659-3_37.

[10] AlDairi, A.—Tawalbeh, L.: Cyber Security Attacks on Smart Cities and Associated Mobile Technologies. Procedia Computer Science, Vol. 109, 2017, pp. 1086–1091, doi: 10.1016/j.procs.2017.05.391.

[11] Komninos, N.—Panori, A.—Kakderi, C.: Smart Cities Beyond Algorithmic Logic: Digital Platforms, User Engagement and Data Science. In: Komninos, N., Kakderi, C. (Eds.): Smart Cities in the Post-Algorithmic Era. Edward Elgar Publishing, 2019, pp. 1–15, doi: 10.4337/9781789907056.00007.

[12] Ahad, M. A.—Paiva, S.—Tripathi, G.—Feroz, N.: Enabling Technologies and Sustainable Smart Cities. Sustainable Cities and Society, Vol. 61, 2020, Art. No. 102301, doi: 10.1016/j.scs.2020.102301.

[13] Dobre, C.—Xhafa, F.: Intelligent Services for Big Data Science. Future Generation Computer Systems, Vol. 37, 2014, pp. 267–281, doi: 10.1016/j.future.2013.07.014.

[14] Hashem, I. A. T.—Chang, V.—Anuar, N. B.—Adewole, K.—Yaqoob, I.—Gani, A.—Ahmed, E.—Chiroma, H.: The Role of Big Data in Smart City. International Journal of Information Management, Vol. 36, 2016, No. 5, pp. 748–758, doi: 10.1016/j.ijinfomgt.2016.05.002.

[15] De Obeso-Orendain, A.—Lopez-Neri, E.—Donneaud-Bechelani, C.: The Role of the Data Scientist Within Smart Cities. IEEE Smart Cities GDL CCD White Paper. Available at: https://smartcities.ieee.org/images/files/pdf/dav_datascientist_v12_final_tjc-eln.pdf.

[16] Chourabi, H.—Nam, T.—Walker, S.—Gil-Garcia, J. R.—Mellouli, S.—Nahon, K.—Pardo, T. A.—Scholl, H. J.: Understanding Smart Cities: An In-

tegrative Framework. 2012 45th Hawaii International Conference on System Sciences, 2012, IEEE, pp. 2289–2297. doi: 10.1109/HICSS.2012.615.

[17] Moustaka, V.—Vakali, A.—Anthopoulos, L. G.: A Systematic Review for Smart City Data Analytics. ACM Computing Surveys (CSUR), Vol. 51, 2019, No. 5, Art. No. 103, doi: 10.1145/3239566.

[18] Khalifa, E.: Smart Cities: Opportunities, Challenges, and Security Threats. Journal of Strategic Innovation and Sustainability, Vol. 14, 2019, No. 3, pp. 79–88, doi: 10.33423/jsis.v14i3.2108.

[19] Braun, T.—Fung, B. C. M.—Iqbal, F.—Shah, B.: Security and Privacy Challenges in Smart Cities. Sustainable Cities and Society, Vol. 39, 2018, pp. 499–507, doi: 10.1016/j.scs.2018.02.039.

[20] Puthal, D.—Mohanty, S. P.—Nanda, P.—Choppali, U.: Building Security Perimeters to Protect Network Systems Against Cyber Threats [Future Directions]. IEEE Consumer Electronics Magazine, Vol. 6, 2017, No. 4, pp. 24–27, doi: 10.1109/MCE.2017.2714744.

[21] Rhee, S.: Catalyzing the Internet of Things and Smart Cities: Global City Teams Challenge. 2016 1st International Workshop on Science of Smart City Operations and Platforms Engineering (SCOPE) in Partnership with Global City Teams Challenge (GCTC, SCOPE-GCTC), 2016, IEEE, pp. 1–4, doi: 10.1109/SCOPE.2016.7515058.

[22] Xie, J.—Tang, H.—Huang, T.—Yu, F. R.—Xie, R.—Liu, J.—Liu, Y.: A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges. IEEE Communications Surveys and Tutorials, Vol. 21, 2019, No. 3, pp. 2794–2830, doi: 10.1109/COMST.2019.2899617.

[23] Sookhak, M.—Tang, H.—He, Y.—Yu, F. R.: Security and Privacy of Smart Cities: A Survey, Research Issues and Challenges. IEEE Communications Surveys and Tutorials, Vol. 21, 2019, No. 2, pp. 1718–1743, doi: 10.1109/COMST.2018.2867288.

[24] Zhang, Y.—Zheng, D.—Deng, R. H.: Security and Privacy in Smart Health: Efficient Policy-Hiding Attribute-Based Access Control. IEEE Internet of Things Journal, Vol. 5, 2018, No. 3, pp. 2130–2145, doi: 10.1109/JIOT.2018.2825289.

[25] Sen, M.—Dutt, A.—Agarwal, S.—Nath, A.: Issues of Privacy and Security in the Role of Software in Smart Cities. 2013 International Conference on Communication Systems and Network Technologies, 2013, IEEE, pp. 518–523, doi: 10.1109/CSNT.2013.113.

[26] Angelidou, M.: The Role of Smart City Characteristics in the Plans of Fifteen Cities. Journal of Urban Technology, Vol. 24, 2017, No. 4, pp. 3–28, doi: 10.1080/10630732.2017.1348880.

[27] Lin, J.—Yu, W.—Zhang, N.—Yang, X.—Zhang, H.—Zhao, W.: A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. IEEE Internet of Things Journal, Vol. 4, 2017, No. 5, pp. 1125–1142, doi: 10.1109/JIOT.2017.2683200.

[28] Sánchez-Corcuera, R.—Nuñez-Marcos, A.—Sesma-Solance, J.—Bilbao-Jayo, A.—Mulero, R.—Zulaika, U.—Azkune, G.—Almeida, A.: Smart Cities Survey: Technologies, Application Domains and Challenges for the Cities of the

Future. International Journal of Distributed Sensor Networks, Vol. 15, 2019, No. 6, doi: 10.1177/1550147719853984.

[29] Cerrudo, C.: An Emerging US (and World) Threat: Cities Wide Open to Cyber-Attacks. Securing Smart Cities, Vol. 17, 2015, pp. 137–151.

[30] Ijaz, S.—Shah, M. A.—Kha, A.—Ahmed, M.: Smart Cities: A Survey on Security Concerns. International Journal of Advanced Computer Science and Applications, Vol. 7, 2016, No. 2, pp. 612–625, doi: 10.14569/IJACSA.2016.070277.

[31] Maciag, M.—Wogan, J. B.: With Less State Aid, Localities Look for Ways to Cope. Governing, The Future of States and Localities, 2017. Available at: https://www.governing.com/archive/gov-state-aid-revenue-sharing-intergovernmental-revenue.html.

[32] Li, T.—Jung, T.—Qiu, Z.—Li, H.—Cao, L.—Wang, Y.: Scalable Privacy-Preserving Participant Selection for Mobile Crowdsensing Systems: Participant Grouping and Secure Group Bidding. IEEE Transactions on Network Science and Engineering, Vol. 7, 2020, No. 2, pp. 855–868, doi: 10.1109/TNSE.2018.2791948.

[33] Ali, B.—Awad, A. I.: Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. Sensors, Vol. 18, 2018, No. 3, Art. No. 817, doi: 10.3390/s18030817.

[34] Ali, S.: Cybersecurity Management for Distributed Control System: Systematic Approach. Journal of Ambient Intelligence and Humanized Computing, Vol. 12, 2021, No. 11, pp. 10091–10103, doi: 10.1007/s12652-020-02775-5.

[35] Anwar, R. W.—Zainal, A.—Abdullah, T.—Iqbal, S.: Security Threats and Challenges to IoT and Its Applications: A Review. 2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC), 2020, IEEE, pp. 301–305, doi: 10.1109/FMEC49853.2020.9144832.

[36] Bhattasali, T.—Chaki, R.—Sanyal, S.: Sleep Deprivation Attack Detection in Wireless Sensor Network. International Journal of Computer Applications, Vol. 40, 2012, No. 15, pp. 19–25, doi: 10.5120/5056-7374.

[37] Fard, S. M. H.—Karimipour, H.—Dehghantanha, A.—Jahromi, A. N.—Srivastava, G.: Ensemble Sparse Representation-Based Cyber Threat Hunting for Security of Smart Cities. Computers and Electrical Engineering, Vol. 88, 2020, Art. No. 106825, doi: 10.1016/j.compeleceng.2020.106825.

[38] Arias, O.—Wurm, J.—Hoang, K.—Jin, Y.: Privacy and Security in Internet of Things and Wearable Devices. IEEE Transactions on Multi-Scale Computing Systems, Vol. 1, 2015, No. 2, pp. 99–109, doi: 10.1109/TMSCS.2015.2498605.

[39] Bellovin, S. M.: Attack Surfaces. IEEE Security and Privacy, Vol. 14, 2016, No. 3, pp. 88–88, doi: 10.1109/MSP.2016.55.

[40] Anwar, R. W.—Bakhtiari, M.—Zainal, A.—Abdullah, A. H.—Qureshi, K. N.: Enhanced Trust Aware Routing Against Wormhole Attacks in Wireless Sensor Networks. 2015 International Conference on Smart Sensors and Application (ICSSA), 2015, IEEE, pp. 56–59, doi: 10.1109/ICSSA.2015.7322510.

[41] Javadzadeh, G.—Rahmani, A. M.: Fog Computing Applications in Smart Cities: A Systematic Survey. Wireless Networks, Vol. 26, 2020, No. 2, pp. 1433–1457, doi: 10.1007/s11276-019-02208-y.

[42] Kirimtat, A.—Krejcar, O.—Kertesz, A.—Tasgetiren, M. F.: Future Trends and Current State of Smart City Concepts: A Survey. IEEE Access, Vol. 8, 2020, pp. 86448–86467, doi: 10.1109/ACCESS.2020.2992441.

Raja Waseem Anwar received his Ph.D. degree from the Universiti Teknologi Malaysia (UTM), Malaysia. Currently he works as Assistant Professor at the Faculty of Computer Studies, Arab Open University, Muscat, Sultanate of Oman. His research interest is in information security, trust and security in wireless sensor networks, cyber physical systems and IoT. Furthermore, he has been involved in organization of many international peer-reviewed conferences, and other scientific events.

Saqib Ali is a business, IT implementation and execution professional, with strong skills in business analysis, software development, management, and implementation, developed through higher education and useful work experience. He has strong understanding of developing business strategies, business process integration and their alignment with IT, along with innovative practices to gain or sustain a competitive advantage. He has also been active in teaching and R & D (Research and Development), he was successful in attracting a number of internal, external and strategic grants while working at the Sultan Qaboos University (SQU). He has published several journal and conference papers, technical reports and edited two books on business information systems. Recently he authored a book on cyber security for cyber physical systems by Springer. In addition, he received a number of awards in teaching, research and academic excellence from SQU. He has been invited to serve in many international conferences, journals and program committees.