Cybersafe Capabilities and Utilities for Smart Cities

Kassim Kalinaki, Navod Neranjan Thilakarathne, Hamisi Ramadhan Mubarak, Owais Ahmed Malik, and Musau Abdullatif

Abstract From the beginning of the 21st century, the entire world suffers from two critical problems: the growth of the world population and the improvement of life expectancy of people owing to the development of healthcare facilities. This has ultimately led to urbanization where a lot of people migrated to cities in search of better prospects. To facilitate those migrating into these cities and with the purpose of better provision of city services, smart cities have emerged thereby connecting everything within the city with the aid of a complex set of technologies. The Internet of Things (IoT) is the fundamental building block of smart cities applied in a variety of smart city solutions, offering real-time information exchange and facilitating ubiquitous connectivity. As IoT is a novel technology that is still in its infancy age and requiring continuous internet connectivity, it paves way for never-ending cyber-attacks targeting smart city services and ultimately endangering the lives of city residents. On the other hand, the security of smart city solutions has always been neglected during the development phase which also endangers the entire city's ecosystem resulting into cyber-attacks from multiple attack vectors. In this chapter,

K. Kalinaki (✉) · M. Abdullatif
Department of Computer Science, Islamic University in Uganda (IUIU), P. O Box 2555, Mbale, Uganda
e-mail: kalinaki@iuiu.ac.ug

N. N. Thilakarathne
Department of ICT, Faculty of Technology University of Colombo, Colombo, Sri Lanka
e-mail: navod.neranjan@ict.cmb.ac.lk

H. R. Mubarak
STEM Education, University of Colorado, Boulder, USA
e-mail: ramadhan.hamisi@colorado.edu

O. A. Malik
School of Digital Science, Universiti Brunei Darussalam, Jalan Tungku Link, BE1410 Bandar Seri Begawan, Brunei Darussalam
e-mail: owais.malik@ubd.edu.bn

M. Ahmed and P. Haskell-Dowland (eds.), *Cybersecurity for Smart Cities*,
Advanced Sciences and Technologies for Security Applications,
https://doi.org/10.1007/978-3-031-24946-4_6

we are providing a brief review of security enhancement capabilities and utilities that can cope with smart cities for the purpose of improving their security against cyber-attacks and safeguarding the privacy of city dwellers.

Keywords Smart city · Cybersecurity · Safety · Privacy · Internet of things · Cybersafe capabilities and utilities

1 Introduction

The technological revolution that began in the early 21st century has fueled the growth of many industries and has introduced many technologies to the world, among which the Internet of Things (IoT) is prominent owing to its ubiquitous connectivity, allowing every digital object to be connected and exchange information [1]. For the time being, the world is undergoing an IoT evolution that connects everything and everyone, allowing for the integration of Information and Communication Technology (ICT) and physical infrastructures (e.g., transportation systems, physical systems, power grids, and so on). This promising connectivity is laying the foundation for making cities smarter by connecting everything within them, including the citizens [1]. The beginning of the 21st century has been impacted by many challenges such as climate challenges, civil and global wars, growing population, urbanization, and disparity in resource allocation [2–4]. On the other hand, at the same time, there was an intensified growth of many digital technologies such as the World Wide Web (WWW) and the Internet. Altogether these challenges and technological revolution have intensified globalization, as to overcome most of the challenges and their adverse consequences leading to an integrated, intelligent, smarter, and sustainable world to make this world a better place [5].

According to the studies [2–6], it is estimated that around 70% of the world population would live in cities by the year 2050 whereas only 13% of the world population lived in cities in 1900. With this rapid urbanization, the world economies have undergone immense pressure to provide necessities that are needed for the survival of citizens in those cities. Energy consumption, public safety, education, transportation, and healthcare facilities were the key resources that have been highly challenged, owing to this rapid urbanization [2]. This continuous pressurization has led to the need for utilizing technology-driven management of cities which paved the way for smart cities [1–5]. In simple terms, a smart city refers to a community that is focused on sustainability, efficiency, and broad participation in decision-making and service provision, which utilizes intensified communication technologies along with IoT as the main backbone. Nevertheless, smart cities have been established in response to the convergence of digital technology and the significant phenomena of community growth and economic innovation that are needed to sustain in the long run.

The IoT being the backbone of the smart city, helps to boost the growth of smart cities by allowing key stakeholders to connect more and more devices, thereby offer-

ing seamless ubiquitous connectivity. The fast growth of IoT services in recent years has driven an ever-increasing rivalry in launching new and creative solutions for smart city applications. In doing so, system developers are often pushed to meet rigorous deadlines to maintain their competitive edge [1–4]. Security and privacy needs are frequently seen as afterthoughts in this rushed development process, to be added to the system afterward as features. As a result, the process produces immature solutions that fail to meet the security and privacy criteria of their intended applications, putting the entire IoT ecosystem and the smart city ecosystem in danger resulting in chaos.

On the other hand, the security and privacy of smart cities have not been treated as an integral and important aspect of smart cities until the large-scale ransomware and distributed denial of service (DDOS) attacks encountered recently, resulting in major worldwide chaos [2]. The consequences of these cyber attacks instilled a sense of suspicion in the IoT, prompting some to accuse it of becoming the Internet of Vulnerabilities [2]. Owing to this mere vulnerable nature, the security and privacy of smart cities are becoming a major concern and many people are interested in discovering innovative ways and solutions to overcoming these ramifications [4–6]. Thus, motivated by the fact that discovering these security and privacy-protective mechanisms protecting smart cities, in the following section we outline the key contributions of this book chapter.

- Following the introduction, in the next section we provide a brief overview of the architecture of a smart city, as it is deemed essential to look into the architecture of a typical smart city before moving into the security and privacy aspect.
- A brief overview of IoT in a smart city is provided, as the backbone of a smart city is made out mostly of IoT, whereas IoT applications in a smart city account for most of the vulnerabilities that exist in smart cities.
- A brief outline of cyber security of the smart cities is provided highlighting the security and privacy aspect of smart cities.
- Following discovery of the cyber security aspect of smart cities next we discuss thoroughly the capabilities and utilities available for enhancing the cyber security of smart cities.
- Finally, the future directions for securing smart cities along with the conclusion will be provided.

The remainder of this chapter is organized as follows. Following the introduction, we provide a brief overview of the architecture of a smart city with a special focus on IoT in Sect. 2 as the IoT constitutes the backbone of a smart city. Next in Sect. 3, we discuss more on the cyber security aspect of smart cities while highlighting security and privacy issues. Thereafter in Sect. 4, we thoroughly discuss the available cybersafe capabilities followed by a comprehensive discussion of cybersafe utilities available for protecting smart cities from cyber threats in Sect. 5. In Sect. 6, we summarize the proposed future security and privacy enhancements of the presented cybersafe capabilities and utilities using blockchain technology and finally, we provide a conclusion of the chapter while highlighting its main strength and weakness.

2 Architecture of a Smart City

The architecture of the smart city is a collation of cyber physical systems (CPS) which are made out of a mixture of digital and physical devices. These CPSs are essentially made out of interconnected physical objects such as a variety of sensing and networking devices for intercommunication. These CPSs in smart cities must do three key tasks: data gathering, determining which operations must be performed, and manipulating physical components [1–5]. In light of CPS, they are prevalently used in various industries such as transportation, energy grids, and healthcare for providing smooth and seamless connectivity and performing real-time operations based on real-time data. On the other hand, according to the studies [4–6], a typical smart city can be apportioned into six dimensions as shown in Fig. 1 [5]. These dimensions are: Smart governance, smart economy, smart living, smart people, smart mobility, and smart environment.

On the other hand, the IoT is a vast network of diverse networked items that have a unique identity and can be referenced using IP or MAC addresses [4–6]. The IoT is a subsidiary of the CPS that is made out of the architecture of the smart city which becomes an integral part of CPS. The IoT devices in smart cities include various sensors used for sensing the environment, actuators, intelligent devices, RFID-enabled devices, and smart mobile devices communicating using de-facto communication protocols. As for the time being, the IoT in smart cities is evolving into a technology that allows for the creation of a system made up of cooperating smart autonomous

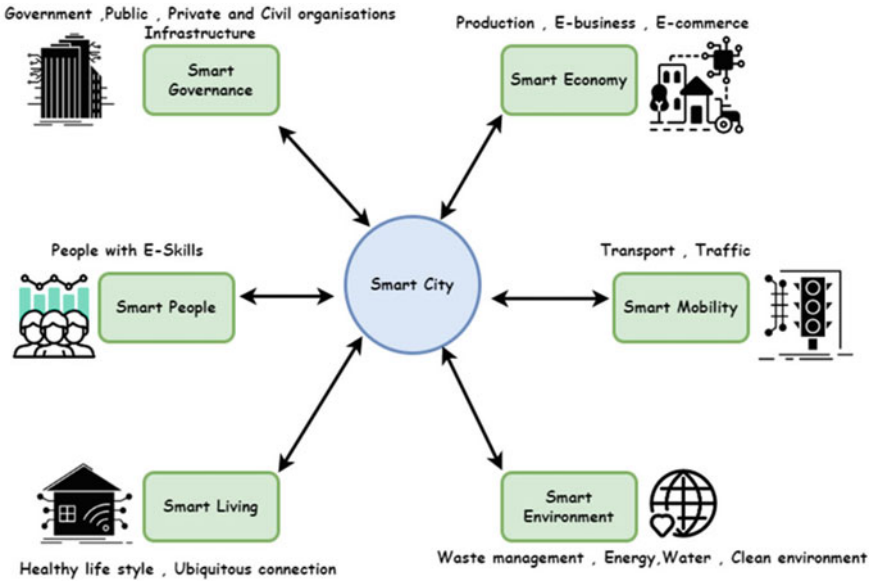

Fig. 1 The six dimensions of a typical smart city

physical-digital devices that are enhanced by sensors and actuators and provide essential processing, storage, and networking capabilities for the smooth operation of smart cities.

In terms of IoT infrastructure used in smart cities apart from sensors and other devices, they consist of communication protocols and APIs (Application Programming Interfaces) used for the collection, aggregation, management, and processing of a large amount of data collated from the city environment which is also known as big data. The implementation might take place on a local or global scale, and it will rely on technologies such as cellular networks, Wi-Fi, and fiber connections for the exchange of data, intercommunication, and connectivity with the Internet. Moreover, cloud computing infrastructures and platforms are also used to deliver flexible cloud-based processing power with big-scale IoT-based CPS.

The underlying communication technologies that provide connectivity to IoT connect the physical city with the data analytics and management units over the Internet. Sensing devices gather data from the city environment, and smart cities modify that data to create a seamless, ubiquitous environment in which data is spread across huge networks and analyzed to produce and give sophisticated intelligent smart services to its people and all stakeholders who are involved in a smart city. According to the studies, it is evident that there is no unique architecture available for smart cities whereas most researchers have referred to the primary IoT architecture as the architecture of the smart city which can be apportioned into three layers; physical layer, network layer, and application layer. For better understanding, the holistic architecture of a typical smart city is presented in Fig. 2 [5].

The physical layer of a typical smart city comprises physical sensing devices which include smart sensing devices, industrial sensors, and wearable devices. These sensors gather data from the physical city and send the gathered data to the processing and, management units in the application layer. These physical sensing devices often belong to the government, private organizations, or individual users. In between the physical and application layer, there is a network layer that is responsible for transmitting gathered data from the physical layer to the application layer with the aid of network infrastructure and underlying communication protocols. The application layer analyzes and processes the obtained sensory data from the physical devices for effective decision-making, using cloud data storage, remote database servers, and specialized control systems. Government institutions, various industries, hospitals, the military, and other approved and authorized bodies have various rights and licenses to examine the underlying information to perform and offer various services.

Further, these institutions will make city-wide rules and regulations based on these inferred data. On the other hand, the smart city also feeds back to alter the actual environment through control and operational components, such as smartphones, based on the decisions made by these processing and management units in the application layer. These control and operational components enhance physical surroundings and improve them to the point where an acceptable quality of life may be achieved in a smart city.

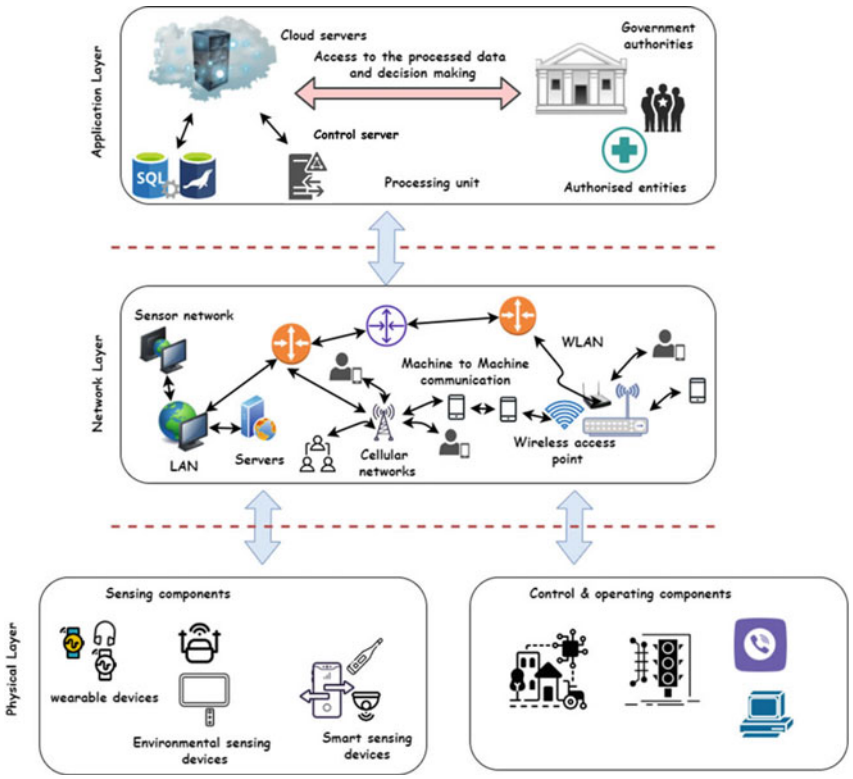

Fig. 2 Architecture of a typical smart city

3 Cyber Security Aspect of a Smart City

Because smart cities are made out of IoT integrated CPS, all the IoT objects in the city are always connected to internal system networks as well as private networks or the internet for real-time exchange of information. This 24/7 connection to the internet always endangers whatever digital devices are connected to the internet in the absence of cyber protection mechanisms. Owing to this vulnerable nature in the absence of cyber security protection mechanism, it would endanger the entire smart city ecosystem where the level of security varies depending on the application and services where the CPS is utilized. Furthermore, the security can also range from physical security to data security while in transmission.

Further, while the smart city applications offer greater flexibility and convenience to city residents, they open up another avenue for malicious cyber-attacks such as system hijacking and Denial of Service (DOS) attacks, jeopardizing every aspect of a smart city. Even though these IoT and associated CPS and eventually the end-user applications offer greater services for city residents, these services often come at a

price, increased risk and vulnerability. Thus, the functioning and the operation of a smart city are subjected to the development and deployment of smart city security solutions. To ensure security, even at a minimal level, the following information security requirements have to be met. These also have to be constantly satisfied while configuring devices, services, and key infrastructure in the smart city.

- **Confidentiality**: This relates to the avoidance of information disclosure to unapproved people, organizations, or systems and protects the underlying infrastructure by preventing unauthorized individuals from accessing the generated data.
- **Integrity**: This is the prevention of falsification, and modification of underlying transmitting network data by unauthorized people or devices, and it includes defense against the manipulation of information by injecting messages, replaying messages, and delaying messages on the network.
- **Availability**: This makes sure that only authorized entities may access data, services, and other resources when they are needed.
- **Authenticity**: This security measure is designed to establish the reliability of a transmission, a message, or its author, or to provide a way of confirming a person's consent to access certain data.

4 Cybersafe Capabilities of a Smart City

Comprehensive IoT security solutions which are simple, practical and yet very secure are required to safeguard connected IoT devices in a typical smart city depicted in Fig. 2 above. Instead of proposing a 'super solution' which may fail to work, these solutions are far more effective and different service providers and original equipment manufacturers (OEMs) can easily and widely deploy them. The following section describes the capabilities of such solutions for the security of smart cities.

4.1 Secure Boot and Firmware Integrity

Secure boot deploys techniques based on cryptographic code signing which guarantees that an IoT device only is capable of executing code generated by the device's original equipment manufacturer (OEM) or a trusted party. This technique ensures the prevention of attacks on the configured IoT devices by refusing to execute the program containing the unsigned malware such as worms, viruses, and pre-boot malware. In the end, hackers are restricted from changing the firmware with any other malicious versions of instruction sets [7].

For smart city devices, a secure boot is a required technological capability that is capable of guaranteeing the integrity and authenticity of software packages and also prevents the unsigned code from being executed [8].

4.2 Security Monitoring, Analysis, and Response

This involves the automated ability of a communications network to collect, record, and monitor various data emanating from several endpoints or locations and connectivity traffic. It also involves the analysis of the collected data for purposes of identifying possible violations of security and assessing the severity of any detected threats to the network. Once threats and violations have been detected, response measures should be instituted in line with the general security policies. Such measures can include but are not limited to: temporarily disabling and isolating the compromised devices, quarantining, or complete disconnection and removal of those devices.

This capability is particularly crucial for smart cities which majorly consist of several interlinked IoT devices that constantly communicate and share end-user data. As stated earlier, these devices are vulnerable to a wide range of attacks across all the layers in the smart city architecture.

4.3 Secure, Mutual Authentication

Different components of a smart city can communicate with each other across different layers of the architecture through various network communication protocols. Therefore, establishing secure communication depends on the integrity, confidentiality, and non-repudiation features of network security [9, 10]. The secure and mutual authentication capability for smart cities guarantees that the communicating entities (IoT device and service) can prove their identities to each other before data transmission takes place. This process legitimizes the device and helps prevent malicious attacks from fraudulent devices connected to the network.

4.4 Security Lifecycle Management

This security capability allows original equipment manufacturers (OEMs) to manage IoT device security aspects during the period of their usage such as during a cyber disaster and unauthorized new services for scrapped IoT devices. Secure device shutdown guarantees that devices that have been scrapped will not be re-used to connect to a service without clearance from the authority. Also, to guarantee minimal service outage and disruption of end-user experience during a cyber incident, rapid over the air (OTA) device key(s) replacement can be adopted [11].

4.5 Updating and Patching

Software packages on IoT devices from OEMs must be periodically updated and the inbuilt security features enhanced to ensure their proper functioning as well as safeguard them from new and sophisticated attacks from multiple attack vectors. Furthermore, updating and patching enable the identification of vulnerabilities by enterprises and the provision of the means through which they can be resolved [8].

5 Cybersafe Utilities for Securing Smart Cities

Without the means to ensure the necessary acceptable level of security and privacy, it would be meaningless to call smart cities smart. The holistic architecture of smart cities shown in Fig. 2 of Sect. 2 above involves several interconnected devices supporting different city-wide services across different layers such as physical, network, and application. These interlinked devices, capable of sharing user data, run different applications with unique vulnerabilities that can be exploited [12]. Any single compromised device can result in the rest of the devices across the network being compromised via several methods such as man-in-the-middle attacks, social engineering, denial of service, unauthorized remote recording, botnets, ransomware, data and identity theft, parameter Tampering attacks, Trojan attacks, data spoofing attacks and buffer overflow attacks among others [13, 14]. This therefore poses serious and unique security requirements which in the long run, prevent the widespread adoption and application of the many services offered in smart cities.

In this section, a detailed discussion of the cyber-safe utilities for enhancing the cybersecurity of smart cities is presented.

5.1 Intrusion Detection System (IDS) and Intrusion Prevention Systems (IPS)

An intrusion detection system is a technique in cybersecurity that is capable of detecting intruders and attacks from multiple attack vectors in any communication system such as in IoT. An intrusion prevention system on the other hand is a network security tool that continuously monitors and secures the network from any sort of malicious attacks sent from specific hosts and takes action to prevent them. Both IDSs and IPSs come in either hardware or software implementations and are crucial to be considered in their integration into the IoT environment to mitigate IoT-related security threats that intend to exploit IoT-related security vulnerabilities [7, 12, 13].

For smart cities, in which IoT devices are vastly deployed, IDSs can be deployed in smart transportation services and specifically connected vehicles. Here, the IDS can filter the data exchanged between various vehicles by detecting any anomalies.

In this case, the IDS prevents attacks associated with connected vehicles such as distributed denial of services (DDOS), timing attacks, Sybil and blackhole among others [15]. The IDS can also be deployed in smart health services such as smart hospitals where they are used to detect unauthorized access to private health records of patients through false data injection (FDI) as well as illegal traffic [16]. Finally, intrusion detection systems have also been deployed in smart homes to detect malicious communication from outside the home network, monitor the home network activities of smart home devices and trigger alerts on detected suspicious or malicious behavior [17, 18].

5.2 Honeypots

A honeypot is defined as a cybersecurity technique designed in a safe and controlled manner to lure attackers into a computer system or network [19]. The hackers, upon successfully breaking into a system, think they have access to the real system and yet it's a decoy made with the sole purpose of being broken into. The owners of the honeypot are then able to study the different attack vectors and other weaknesses through which attacks can be made on the real system. In smart home systems, the YAKSHA honeypot is often deployed to collect data for analysis and report information regarding the status of the YAKSHA smart installations system. In so doing, it has shown great success in providing good insights on actual attacks that were launched on a home smart system [20].

Several honeypots such as honeyd, honeydv6, conpot, CryPLH, Supervisory Control and Data Acquisition (SCADA), HoneyNet Project, and SHaPe have been explored for purposes of securing smart grids and industrial control systems (ICS) [21]. All of those honeypots have been used in identifying attacks, gathering intelligence on attack strategies as well as misleading hackers from attacking and causing damage to the smart grid infrastructure. Furthermore, the ZigBee honeypots have been implemented in several profiles for smart health, smart energy, smart agriculture, and smart homes through several standards and specifications intended for short-range wireless technologies [22]. Finally, several honeypots have been applied in water systems with varying levels of interaction (low, medium, high and hybrid) which simulated several services such as transmission control protocol (TCP), EtherNet/Internet Protocol (IP), Hypertext Transfer Protocol (HTTP), and File Transfer Protocol (FTP) [19].

5.3 Demilitarized Zone (DMZ)

A demilitarized zone (DMZ) serves as a perimeter network commonly deployed on an organization's border to protect its internal local area network (LAN) from untrusted traffic. As the network expands with time, it is recommended for any large network to

create a perimeter security network such as a DMZ to separate the internal network from the outside untrusted world. Typically, DMZ houses internal resources such as web servers, e-mail servers, domain name servers (DNS) and other systems that have some level of accessibility from the outside world. The resources in DMZ have limited LAN access with an interest to ensure that one can only access them via the public network rather than internal LAN [23]. This, therefore, makes it challenging for hackers to gain direct access to internal systems and sensitive organization data.

In smart cities, a DMZ can be deployed in smart healthcare to separate public resources (such as patient application systems) from internal sensitive information (internal network) and thereby protecting patients' records from being accessed by untrusted traffic [24]. Real-life smart city endeavors such as the Aspern smart city research project in Vienna, Austria have demonstrated the application of demilitarized zones to restrict which services have a higher likelihood of exposure to external entities. For instance, users in such a smart city should have access to the directory containing application programming interfaces (APIs) but be restricted from access to specific APIs via a firewall implementation [25].

5.4 Firewalls

Firewalls (software or hardware) are used to monitor all incoming and outgoing traffic to allow "good data" in, but deny or block "bad data" from entering into a device or network. They act as the first line of defense and gatekeeper for all sorts of traffic flowing in and out of a network [26, 27]. Cloud-based firewalls can be configured in a smart healthcare environment to reduce the impact of cyber threats and safeguard cyber-attacks against smart healthcare devices that carry sensitive data and information [27]. Much as global positioning systems (GPS) and vehicular ad hoc networks (VANET) have long been used for the integrity and overall performance of vehicular networks in big cities, firewalls can also be incorporated to secure the smart transportation system and be free from security breach and jamming of the transportation network [28]. Finally, the firewall can also be deployed in a Smart Home system that uses IoT devices such as smart thermostats, cameras, speakers, toothbrushes, and so on to restrict their access by allowing certain traffic and blocking untrusted access from commanding and controlling IoT devices by unauthorized user [29].

In the table below, we present a summary of cybersafe utilities for securing smart cities (Table 1).

Table 1 Summary of the cybersafe utilities

Utility	Smart city dimensions secured	Articles
Intrusion detection systems (IDSs) and Intrusion Prevention Systems (IPSs)	Smart transportation, smart healthcare and smart homes	[15–18]
Honeypots	Smart homes, smart grids, water systems and smart agriculture	[19–22]
Demilitarized zones	Smart healthcare, an entire smart city	[24, 25]
Firewalls	Smart healthcare, smart transportation, smart homes	[27–29]

6 Future Directions

Owing to their abilities to offer intelligent services such as smart transportation, smart grids, smart healthcare, smart homes, smart agriculture, and smart banking, to mention but a few, the implementation of smart cities is not yet widespread mainly due to numerous security-related concerns which have been partly addressed by the above cyber safe utilities and capabilities. The above services run sophisticated applications that require enhanced security capable of handling the huge amounts of data in the smart city network while at the same time improving the quality of the city dwellers' lives. However, many IoT-related security issues are still unresolved in smart cities and the current technologies and methods are unable to fully address them. In this section, a discussion of the future direction for securing smart cities is provided through the adoption of Blockchain technology which has good security enhancements, especially for IoT.

Defined as a decentralized, transparent, traceable & immutable ledger consisting of transnational records in Peer-to-Peer networks [30], blockchain is considered as a solution capable of enhancing security and privacy in smart cities [31]. In its initial stages, blockchain rose to fame as bitcoin whose solution was for the decentralized transfer of digital payments among different parties [32]. In addition to financial sector improvement, there are several applications where blockchain has potential. Fields like the internet of things (IoT), identity management, accounting and auditing, supply chain, healthcare, telecommunications, energy, and several government public services [33] are some of those in which blockchain is applied.

The table below summarizes the proposed security and privacy enhancements for smart city services using blockchain (Table 2).

Table 2 Summary of the proposed security and privacy enhancements for smart city services using blockchain

Smart city service	Proposed blockchain-enabled security and privacy solution / framework / Protocol / Prototype	Brief description	Articles
Smart e-commerce	Proof of Delivery (PoD) framework	This framework deploys Ethereum smart contracts and blockchain technologies allowing for a secure and transparent logistics control and management of tangible assets either between intermediary transporters or through the sole carrier	[34]
Smart e-commerce	Dual-Deposit escrow protocol	This protocol helps in solving the buyer and Seller's dilemma for selling a digital good in which case the dilemma entails the matter of trust for payment as well as genuine digital goods delivery	[35]
Smart transportation	Blockchain-based Intelligent transportation system (B-ITS) framework	Without technical details for real-world smart city implementation, this proposed framework employs a seven-layered blockchain configuration for securing vehicular networks in smart cities. The layers include the physical, data, network, consensus, incentive, contract, and finally the application layer	[36]
Smart healthcare	MedRec	This is a blockchain-based prototype aimed at providing the means through which e-health records are securely stored for medical research. This prototype is capable of addressing patient privacy together with ensuring improved quality and quantity of medical research data. Modification of medical records in this prototype is prevented through a cryptographic hash application	[37]

(continued)

Table 2 (continued)

Smart city service	Proposed blockchain-enabled security and privacy solution / framework / Protocol / Prototype	Brief description	Articles
Smart grid	Blockchain as a cyber layer, agent/aggregator-based microgrid blockchains, and application-specific blockchains	All those security solutions are capable of providing security and privacy in smart city power grids through the applications of cryptographic securitization together with the consensus mechanism. These ensure data immutability already contained in the blockchain	[38]
Smart home	Homomorphic consortium blockchain model for sensitive data privacy-preserving (HCB-SDPP)	This blockchain-based framework was proposed for the smart home system (SHS) to enhance security and privacy through the application of the Paillier encryption mechanism. Upon analyzing its performance, the framework was determined to be very robust, especially in terms of data availability, data security, and ledger storage security	[39]

7 Conclusions

In this chapter, we have outlined a discussion on capabilities and utilities available for enhancing the cyber security of smart cities along with a summary of key future technologies, from our point of view. As the cyber-attacks targeting internet-facing devices are increasing rapidly, the residents and the relevant stakeholders must act immediately to cover up the vulnerabilities and implement or adapt the cyber security capabilities and utilities towards mitigating unforeseen cyber threats.

The major strength of this chapter lies in the fact that the capabilities and utilities presented can easily and widely be adopted by cyber security specialists, service providers and original equipment manufacturers (OEMs) in their quest to ensure the security and privacy of users in smart cities. One key weakness however lies in the inadequate real-life implementations of some of the summarized future technologies for enhancing the security of smart cities using blockchain. This weakness is attributed to the slow-paced implementation of smart cities worldwide which in turn yields less information on the effectiveness and vulnerabilities of the proposed security enhancements.

In summary, through our discussion, what we have understood is security should be an integral part of a smart city and the developers and architects should put more concerted efforts when designing smart city solutions. We believe this chapter would be an ideal guide for researchers and relevant stakeholders who are keen on this area.

References

1. Jin D, Hannon C, Li Z, Cortes P, Ramaraju S, Burgess P, Buch N, Shahidehpour M (2016) Smart street lighting system: a platform for innovative smart city applications and a new frontier for cyber-security. Electr J 29(10):28–35
2. Habibzadeh H, Nussbaum BH, Anjomshoa F, Kantarci B, Soyata T (2019) A survey on cyber-security, data privacy, and policy issues in cyber-physical system deployments in smart cities. Sustain Cities Soc 50:101660
3. Khan F, Kumar RL, Kadry S, Nam Y, Meqdad MN (2021) Cyber physical systems: a smart city perspective. Int J Electr Comput Eng 11(4):3609
4. ABDOULLAEV A (2011) A smart world: A development model for intelligent cities-[the trinity world of trinity cities]. EIS Encyclopedic Intelligent Systems/SMART GROUP
5. Thilakarathne NN, Madhuka Priyashan W (2022) An overview of security and privacy in smart cities. IoT and IoE Driven Smart Cities, pp 21–44
6. Elhoseny M, Thilakarathne NN, Alghamdi MI, Mahendran RK, Gardezi AA, Weerasinghe H, Welhenge A (2021) Security and privacy issues in medical internet of things: overview, countermeasures, challenges and future directions. Sustain 13(21):11645
7. Singh D, Pati B, Panigrahi CR, Swagatika S (2020) Security issues in iot and their countermeasures in smart city applications. Advanced Computing and Intelligent Engineering. Springer, pp 301–313
8. Sookhak M, Tang H, He Y, Yu FR (2018) Security and privacy of smart cities: a survey, research issues and challenges. IEEE Commun Surv & Tutor 21(2):1718–1743
9. Liu N, Chen J, Zhu L, Zhang J, He Y (2012) A key management scheme for secure communications of advanced metering infrastructure in smart grid. IEEE Trans Ind Electron 60(10):4746–4756
10. Khalil U, Malik OA, Hussain S et al (2022) A blockchain footprint for authentication of iot-enabled smart devices in smart cities: State-of-the-art advancements, challenges and future research directions. IEEE Access 10:76 805–76 823
11. Halder S, Ghosal A, Conti M (2020) Secure over-the-air software updates in connected vehicles: a survey. Comput Netw 178:107343
12. Butt TA, Afzaal M (2019) Security and privacy in smart cities: issues and current solutions. Smart technologies and innovation for a sustainable future. Springer, pp 317–323
13. Alli AA, Kassim K, Mutwalibi N, Hamid H, Ibrahim L (2021) Secure fog-cloud of things: architectures, opportunities and challenges. Secure edge computing, pp 3–20
14. Khalil U, Malik OA, Uddin M, Chen C-L (2022) A comparative analysis on blockchain versus centralized authentication architectures for iot-enabled smart devices in smart cities: a comprehensive review, recent advances, and future research directions. SensS 22(14):5168
15. Aloqaily M, Otoum S, Al Ridhawi I, Jararweh Y (2019) An intrusion detection system for connected vehicles in smart cities. Ad Hoc Netw 90:101842
16. Saba T (2020) Intrusion detection in smart city hospitals using ensemble classifiers. In: 2020 13th International Conference on Developments in eSystems Engineering (DeSE)
17. Kesswani N, Agarwal B (2020) Smartguard: an iot-based intrusion detection system for smart homes. Int J Intell Inf Database Syst 13(1):61–71
18. Alsakran F, Bendiab G, Shiaeles S, Kolokotronis N (2019) Intrusion detection systems for smart home iot devices: experimental comparison study. In: International Symposium on Security in Computing and Communication. Springer, pp 87–98

19. Franco J, Aris A, Canberk B, Uluagac AS (2021) A survey of honeypots and honeynets for internet of things, industrial internet of things, and cyber-physical systems. IEEE Commun Surv & Tutor 23(4):2351–2383
20. Kostopoulos A, Chochliouros IP, Apostolopoulos T, Patsakis C, Tsatsanifos G, Anastasiadis M, Guarino A, Tran B (2020) Realising honeypot-as-a-service for smart home solutions. In: (2020) 5th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM). IEEE, pp 1–6
21. Dalamagkas C, Sarigiannidis P, Ioannidis D, Iturbe E, Nikolis O, Ramos F, Rios E, Sarigiannidis A, Tzovaras D (2019) A survey on honeypots, honeynets and their applications on smart grid. In: 2019 IEEE Conference on Network Softwarization (NetSoft). IEEE, pp 93–100
22. Dowling S, Schukat M, Melvin H (2017) A zigbee honeypot to assess iot cyberattack behaviour. In: (2017) 28th Irish signals and systems conference (ISSC). IEEE, pp 1–6
23. Nadig D, Ramamurthy B (2019) Securing large-scale data transfers in campus networks: experiences, issues, and challenges. In: Proceedings of the ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization. pp 29–32
24. Ahmed SM, Rajput A (2020) Threats to patients' privacy in smart healthcare environment. Innovation in Health Informatics. Elsevier, pp 375–393
25. Dhungana D, Engelbrecht G, Parreira JX, Schuster A, Valerio D (2015) Aspern smart ict: data analytics and privacy challenges in a smart city. In: (2015) IEEE 2nd World Forum on Internet of Things (WF-IoT). IEEE, pp 447–452
26. van Oorschot PC (2021) Firewalls and tunnels. Computer security and the internet. Springer, pp 281–308
27. Anwar RW, Abdullah T, Pastore F (2021) Firewall best practices for securing smart healthcare environment: a review. Appl Sci 11(19):9183
28. Jain N, Panda S, Agrawal H (2014) Smart firewall integrated intelligent transportation system for security in ubiquitous computing. Int J Emerg Technol Adv Eng 4(1):684–689
29. Haar C, Buchmann E (2019) Fane: a firewall appliance for the smart home. In: 2019 Federated Conference on Computer Science and Information Systems (FedCSIS). IEEE, pp 449–458
30. Yaqoob I, Salah K, Uddin M, Jayaraman R, Omar M, Imran M (2020) Blockchain for digital twins: recent advances and future research challenges. IEEE Netw 34(5):290–298
31. Biswas K, Muthukkumarasamy V (2016) Securing smart cities using blockchain technology. In: (2016) IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS). IEEE, pp 1392–1393
32. Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system. Decentralized Business Review, p 21260
33. Majeed U, Khan LU, Yaqoob I, Kazmi SA, Salah K, Hong CS (2021) Blockchain for iot-based smart cities: recent advances, requirements, and future challenges. J Netw Comput Appl 181:103007
34. Hasan HR, Salah K (2018) Proof of delivery of digital assets using blockchain and smart contracts. IEEE Access 6:65 439–65 448
35. Asgaonkar A, Krishnamachari B (2019) Solving the buyer and seller's dilemma: a dual-deposit escrow smart contract for provably cheat-proof delivery and payment for a digital good without a trusted mediator. In: 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE, pp 262–267
36. Yuan Y, Wang F-Y (2016) Towards blockchain-based intelligent transportation systems. In: (2016) IEEE 19th international conference on intelligent transportation systems (ITSC). IEEE, pp 2663–2668
37. Azaria A, Ekblaw A, Vieira T, Lippman A (2016) Medrec: using blockchain for medical data access and permission management. In: (2016) 2nd international conference on open and big data (OBD). IEEE, pp 25–30
38. Musleh AS, Yao G, Muyeen S (2019) Blockchain applications in smart grid–review and frameworks. Ieee Access 7: 86 746–86 757
39. She W, Gu Z-H, Lyu X-K, Liu Q, Tian Z, Liu W (2019) Homomorphic consortium blockchain for smart home system sensitive data privacy preserving. IEEE Access 7:62 058–62 070