Security and Privacy of Smart Cities: A Survey, Research Issues and Challenges

Mehdi Sookhak, Helen Tang, *Senior Member, IEEE*, Ying He, *Student Member, IEEE*, and F. Richard Yu, *Fellow, IEEE*

***Abstract*—With recent advances of information and communication technology, smart city has been emerged as a new paradigm to dynamically optimize the resources in cities and provide better facilities and quality of life for the citizens. Smart cities involve a variety of components, including ubiquitous sensing devices, heterogeneous networks, large-scale databases, and powerful data centers to collect, transfer, store, and intelligently process real-time information. Smart cities can offer new applications and services for augmenting the daily life of citizens on making decisions, energy consumption, transportation, healthcare, and education. Despite the potential vision of smart cities, security and privacy issues remain to be carefully addressed. This paper delineates a comprehensive survey of security and privacy issues of smart cities, and presents a basis for categorizing the present and future developments within this area. It also presents a thematic taxonomy of security and privacy issues of smart cities to highlight the security requirements for designing a secure smart city, identify the existing security and privacy solutions, and present open research issues and challenges of security and privacy in smart cities.**

***Index Terms*—Smart cities, security, privacy, Internet of Things, cloud computing, big data.**

I. Introduction

NOWADAYS, more than 54 percent of the world's population are living in urban areas, and by 2050, it is predicted that this rate will reach 66 percent [1]. The rapid population growth along with the increased urbanization have raised a variety of technical, social, economic, and organizational problems, which tend to endanger the economical and environmental sustainability of cities. Hence, the majority of governments have been taking an interest in adopting "smart" concepts, for optimizing the use and exploitation of both tangible (e.g., transport infrastructures, energy distribution networks, and natural resources) and intangible assets (e.g., human capital, intellectual capital of companies, and organizational capital in public administration bodies) [2].

The "smart city" concept refers to applying all available technology and resources in an intelligent and coordinated manner with the aim of developing urban centers that are at once integrated, habitable, and sustainable [3]. The smart city has great applications in the modern societies, such as: smart energy for optimizing the generation, monitoring, and consumption of different types of energy and resources by using digital technologies; smart building for independently controlling and managing the lighting and temperature system, security, and energy consumption throughout the large constructions; smart mobility for enabling intelligent mobility by utilizing the innovative and integrated technologies and solutions; smart technology for enabling intelligent network connectivity and edge processing solutions in cities across the globe; smart health-care for enabling intelligent systems and connected medical devices to promote wellness, provide health monitoring and diagnostics; smart governance and education to provide policies and digital services from the government and facilitate the educational system through the modern technologies; smart security for reducing the security risks and managed security services to protect people, properties, and information [4], [5].

Frost & Sullivan recently reported that the smart cities' market is expected to be worth a cumulative $1.5 trillion by 2020 [6]. In fact, the governments have to pay more attention to attract huge investments for upgrading old-economy cities and fulfilling the vision of the smart city [7], [8]. This enormous retrofitting consists of deploying hundreds of thousands of sensor nodes in a city to feed big data city management systems and commercial applications, which provide the real-time information to citizens about traffic flows, available parking space availability, arrival times of public transportation, the quality of air and water, the rate of energy consumption, and developing emergencies [9]. However, generating, processing, analyzing, sharing, and storing the huge volume of sensitive data raise a number of concerns and challenges about security and privacy of data and how to protect them against unauthorized parties during different steps [10]–[14].

Constructing a smart city to deliver many valuable time saving and resource saving conveniences requires higher degrees of network connectivity to support new sophisticated features, which results in increasing concerns about security and privacy [9], [15]. The existing Internet of Thing (IoT) devices,

Manuscript received August 15, 2017; revised March 16, 2018 and June 3, 2018; accepted July 7, 2018. Date of publication August 27, 2018; date of current version May 31, 2019. This work was supported in part by the Natural Sciences and Engineering Research Council of Canada and in part by the Defence Research and Development Canada. *(Corresponding author: Ying He.)*

M. Sookhak is with Polytechnic School, Arizona State University, Tempe, AZ 85287 USA.

H. Tang is with the Centre for Security Science, Defence Research and Development Canada, Ottawa, ON K1A 0K2, Canada.

Y. He and F. R. Yu are with the Department of Systems and Computer Engineering, Carleton University, Ottawa, ON K1S 5B6, Canada (e-mail: heying@sce.carleton.ca).

Digital Object Identifier 10.1109/COMST.2018.2867288

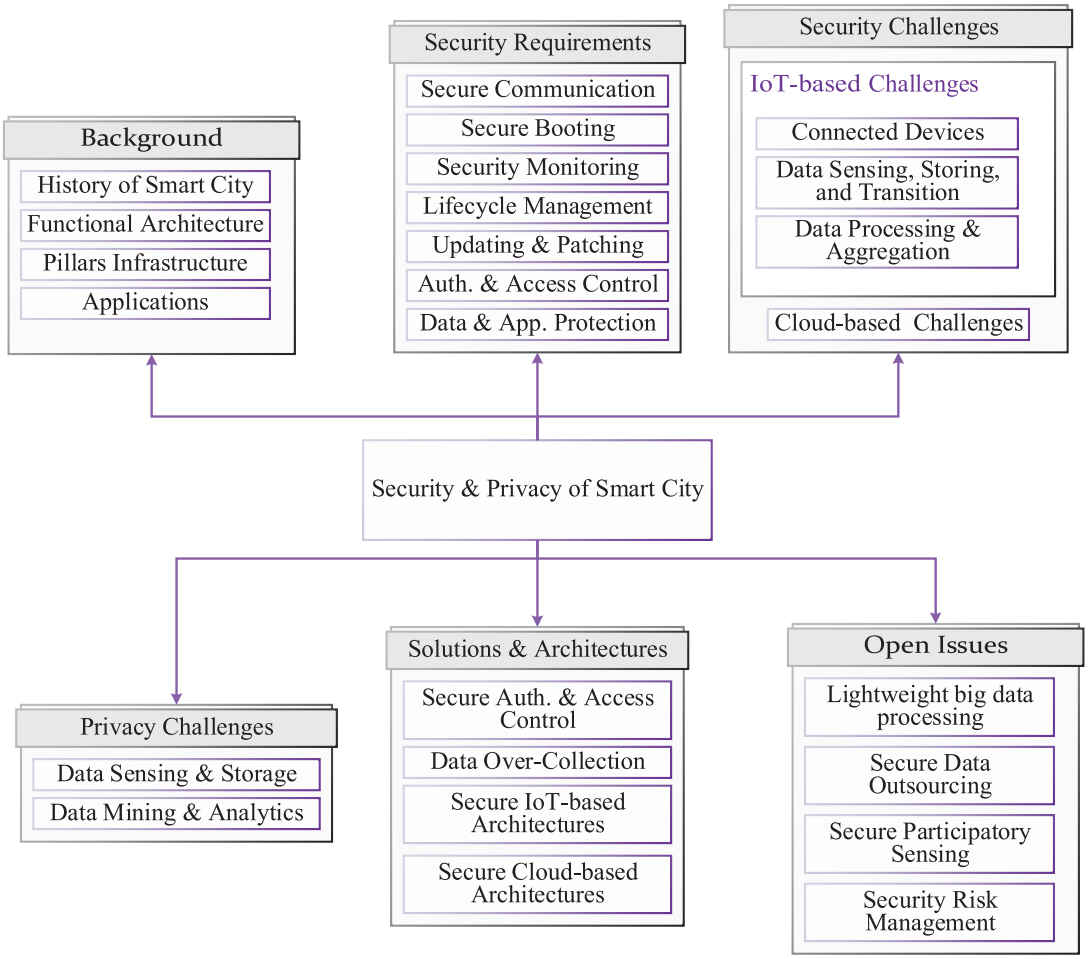

Fig. 1. Roadmap of security and privacy of smart cities.

which are responsible to collect the data from diverse resources and transfer them to the storage centers through the existing networks, extend the attack surface and create a potential entry point for malicious attackers to intrude into the system. Moreover, the malicious node and devices are able to lunch different types of attacks, such as denial-of-service, eavesdropping, Structured Query Language (SQL) injection, session hijacking, and brute-force attack to reduce the quality of intelligent services in smart cities. The cities also have numerous pervasive video surveillance systems and Global Positioning System (GPS) for collecting high sensitive data, which may be used by attackers to identify citizens trajectory and fundamentally endanger their privacy. Albeit some of the existing security algorithms might be applicable in smart cities, the majority of them are not able to efficiently protect the security and privacy of data in the smart cities to due to collecting, storing, and real-time analyzing of huge volume of data. In addition, the emergence of some smart attacks, such as side channel attack and cold boot attack, which can disrupt the citizens privacy, makes it essential to design the appropriate security methods for smart cities [10], [16].

This paper delineates an extensive survey of security and privacy issues of smart cities, and presents a basis for categorizing the present and future developments within this novel area. The core contributions of the survey are (i) the review of the existing security and privacy requirements, issues, and challenges of smart cities with the aim of identifying the open issues and challenges that can be used as a future direction, and (ii) analysis and classification of current security and privacy solutions of the smart cities into two different categories, such as IoT-based and cloud-based solutions on the basis of their architectures and applications. In addition, we explore the similarities and differences of such solutions that have not been appropriately covered in the literature to diagnose the significant and outstanding open issues for further studies.

Fig. 1 illustrates a comprehensive roadmap of our approach and taxonomizes the security and privacy of smart cities on the basis of following attributes: (i) Smart city background makes an overview on the history of smart city and presents a general architecture for smart cities; (ii) Security requirements: indicates the necessary components to design a secure smart city, such as secure communication, booting, and monitoring, life style management, data protection (e.g., confidentiality, integrity and availability), and identification and data access control; (iii) Security threats: refer to the list of the intentional and unintentional issues and challenges in different layers of the IoT-based and cloud-based smart city architectures (e.g., sensing, transferring, storing, and processing

layers), which can be used by unauthorized party to attack the system; (iv) Privacy challenges: generally, privacy debates concern acceptable practices considering with accessing and revealing personal and sensitive information of the citizens during data sensing and data analysis process; (v) Security solution: shows the possible solutions to cope with the existing security and privacy issues and challenges; and (vi) Open issues that indicate some issues that have not been addressed properly and can be used by researchers as a future direction.

We have done a computer-assisted literature search through some databases: IEEE Xplore Digital Library, Springer, Science Direct (Elsevier), Wiley Online Library, the IET library, Sage journals library, and Scopus. Since there are some useful technical report about smart cities, we find them by using the Google search engine. We have leveraged a combination of some keywords to search for finding the relevant studies about smart cities: security and privacy/ smart city/ IoT/ big data/ cloud/ cloud of things/fog and edge.

The organization of the remainder of the paper is as follows: Section II makes a historical overview on the smart city concept in which the main features of three different types of cities, such as digital cities, information and communication technology (ICT) cities, and compound cities, are critically presented. It also describes the core components, pillars, and applications of smart cities. Section III elaborates the essential prerequisites to design a secure smart city. Sections IV and V discuss the security and privacy issues and challenges of the smart cities. Section VI presents an extensive review of the most-recent security solutions for smart cities and investigates their strengths and weaknesses. Section VII explains the open issues and challenges within the contemporary smart cities. Finally, Section VIII concludes the paper and explains some future research directions. Table I presents the list of acronyms used in the paper.

TABLE I
LIST OF ACRONYMS

Symbol	Description
ABE	Attribute-based encryption
AES	Advanced Encryption Standard
CapBAC	Capability-Based Access Control
CCTV	Closed-circuit television
CSP	Cloud Service Provider
CSRF	Cross-Site Request Forgery
DCapBAC	Distributed Capability-Based Access Control
DDoS	Distributed Denial of Service
EAPOL	Extensible Authentication Protocol Over LAN
ECC	Elliptic Curve Cryptography
ECCDH	Elliptical Curve Cryptography-Diffie Hellman
EULA	End-user license agreements
GCD	Governmental Control Domain
GPS	Global Positioning System
IBE	Identity-Based Encryption
ICAC	Identity driven Capability based Access Control
ICAP	Identity-based Capability
ICT	information and communication technology
ID	Identity document
IECAC	Identity Establishment and Capability-based Access Control
IMEI	International Mobile Station Equipment Identity
IoT	Internet of Thing
JSON	Java Script Object Notation
LIBC	Lightweight Identity Based Cryptography
LR-WPAN	Low-Rate Wireless Personal Area Networks
MAC	Message Authentication Code
MARS	Monitoring, Analysis, and Response System
MEID	Mobile Equipment Identifier
OFB	Output Feedback Mode
OS	Operating System
PDP	Policy Decision Point
PEP	Privacy Enforcement Points
RBAC	Role-Based Access Control
RDA	Remote Data Auditing
SDN	Software Defined Network
SLA	Service Level Agreement
SQL	Structured Query Language
UDID	Unique Device Identifier
UPECSI	User-driven Privacy Enforcement for Cloud-based Services
VM	Virtual Machine
XACML	Extensible Access Control Markup Language
XSS	Cross-site scripting

II. BACKGROUND OF SMART CITY

This section presents a brief history of smart city concept and critically reviews the existing definitions. It also describes the important components of functional architecture, pillars infrastructure, and the existing applications of smart cities.

A. The History of Smart City

Over the last decade, developing the modern technology directs the cities in the smart environment, which consents cites to intelligently optimize the scarce resources, save money, and provide pervasive resources for all citizens. The fantastic outcomes of the smart cities have motivated a huge number of researchers to focus on promoting and developing new smart city solutions. However, there is no unique and well delineated definition for the smart city concept.

In the existing literature, there are three main visions for smart cities, such as digital cities, ICT cities, and compound cities based on the combination of earlier technological deployments (e.g., wired cities and digital cities) with current city framings (e.g., resilient cities, safe cities, and eco-cities) [17]. In the following, we briefly describe these conceptions.

In the first vision, smart cities refer to digitally instrumenting cities for modifying the way that urban infrastructures and city services are managed. The main component of smart cities in this viewpoint is digitally-enabled devices that are embedded into the fabric of cities, such as smart meters, software-controlled equipment, sensors, and digital CCTVs. They are responsible for producing a huge volume of continuous data streams that are used to control the real-time regulation of city systems, such as transportation systems, home and environment, energy supply, and security and emergency services [18]. Furthermore, this type of data provides a great opportunity to perform further urban development by simulating the existing models and identify the possible issues [19], [20].

The next group considers smart cities as plans for developing and improving urban policies by applying advances in ICT to reconstruct human capital, creativity, and innovation and produce smarter citizens, workers and public services [21]. In other words, the smart city exploits e-government, produces open data and cultivates open data economy, creates

TABLE II
CATEGORIZING SMART CITY DEFINITIONS

Type	Ref.	Key Features
Digital City	[24]	Connecting people and city elements to gather information for creating a sustainable, greener city using new technologies
	[25]	Optimizing electrical resources, transportation, and other city operations using the deployed sensors and communication systems
	[26]	Interconnecting physical, IT, social, and business infrastructures to achieve intelligent city
	[27]	An effective solution to control the resources
ICT City	[28]	Investing in human and social capital and ICT communication to manage natural resources
	[29]	Using smart communities to achieve an ideal economy and society and increase quality of life
	[30]	Exchanging and analyzing information intelligently on the basis of a smart governance operating for achieving sustainable city
	[31]	Identifying economy, people, governance, mobility, environment and living as the main characteristics of smart city
	[32]	Promoting socio-economic, ecological, logistic and competitive performance of cities by applying knowledge-intensive strategies
Compound City	[33]	Applying ICT to promote human, social, relational, and environmental capitals
	[3]	Developing urban centers (economic, human, social, and environmental capitals) using all available technology and resources
	[34]	Including everything related to either governance and economy, or ICT, sensors, smart devices, and real-time data analysis city
	[35]	Cultivating socio-technical and socio-economic aspects of cities by using specific intellectual abilities
	[36]	Applying ICT to optimize resources and infrastructures, augment economy capitals

citizen-center databases to store city performance, provides a testbed to check the effectiveness of urban services, and fosters the utilization of ICT in educational activities [14].

Finally, in the third vision of smart city, both digital technologies and ICT are used to augment a citizen-centric model of urban development and management results in improving social innovation, social justice, and transparency and accountable governance [18]. In other words, a smart city helps to augment a smart society for serving local communities and reducing discriminations. This concept mainly focuses on crowd sourcing and communal action; open source platforms, software and data; and digital and data literacy [14].

On the other hand, the visions, ambitions, and drivers of smart cities may depend on the geographical location [22], [23]. For example, the main goals of smart city in the developed countries are usually promoting the efficiency of services and creating resilience and sustainability, while the developing countries are looking for managing economic and urban transitions, improving modernization and national development, and answering to population growth. Table II presents the key features of some of the existing smart city definitions.

B. Functional Architecture of Smart Cities

The smart cities usually have a unique architecture, which consists of four distinct layers with specific responsibilities and components, as follows:

1) Sensing Layer: As the first layer of smart city architecture, is comprised of different component and instruments to collect data from surrounding environment, for example, different type of sensors, actuators, and cameras. The sensor nodes have to be deployed in diffract sections of smart cities to collect and deliver data to the data collection layer.

2) Data Collection Layer: After collecting data from the different resources of the smart cities, such as homes, traffics, and citizens, it requires to transmit them using reliable wired or wireless communication to the local databases, which are responsible for storing the collected data. However, storing such big volume of data incurs high storage overhead on the existing databases of this layer. Although the majority of architectures use the remote cloud storage systems to address this issue, we need the effective data parsing algorithms to filter the data, build the useful data context, and alleviate the large-scale issue of collected data.

3) Data Processing Layer: The stored in local or remote databases of data collection layer has to be delivered to the data processing layer to perform per-processing techniques on the basis of the smart city applications. For example, real time processing (online event processing) and batch processing are two most important components of this layer, which usually deals with high volume of data. However, it is impossible to process and manage the collected big data by using the traditional algorithms (e.g., the majority of data mining methods), which are only applicable for normal data with limited and well-defined data sets. As a result, it is essential to design complex and sophisticated algorithms that have the capability to effectively process high volumes of data with a large variety in heterogeneous and dynamic environment. Moreover, to reduce the latency in delay-sensitive applications, it is possible to perform the per-processing step at the edge of the network (fog computing).

4) Smart Processing & Application Layer: As one of the main layers of smart city architecture is responsible for exchanging data between operators (e.g., citizens and stockholders) and smart applications. This layer can also perform an accurate data analysis for making global decision and deliver raw data for the smart cities applications. The main difference between smart processing and data preprocessing layers is about the application of data processing layer for carrying out the real-time data analysis.

Fig. 2 shows the functional architecture of smart cities along with the important components of each layer.

C. Pillars Infrastructure

There are four fundamental infrastructures, which are known as pillars of smart cities [37], [38], as follows.

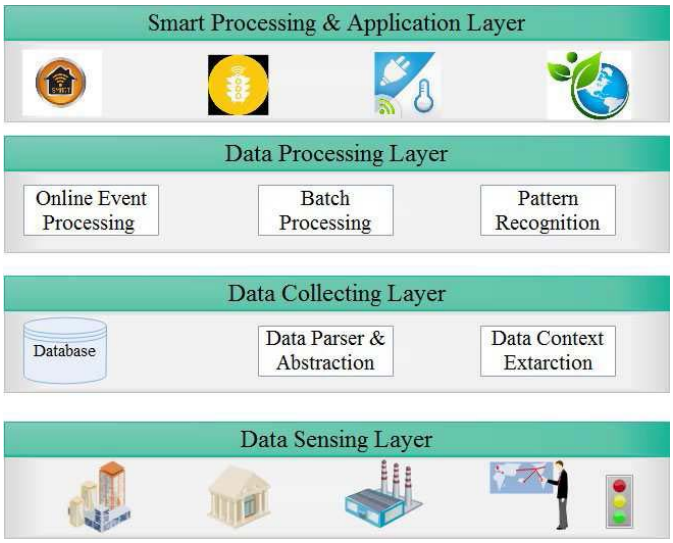

Fig. 2. Functional architecture of smart cities.

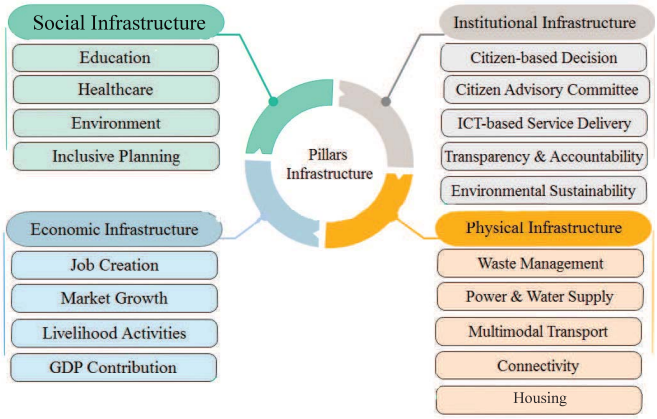

Fig. 3. Smart city pillars.

1) Institutional Infrastructure: Pertains to the fundamental activities, such as management, governance, and planning of a city with the aim of including citizens in decision-making processes. To ensure that such decisions are taken without any arbitrariness and discrimination, it is essential to process the information on the real-time basis under a comprehensive Service Level Agreements (SLA) [37]. Moreover, ICT helps to provide an efficient, accountable and transparent citizen-centric system.

2) Physical Infrastructure: Indicates applying ICT to integrate the cost-efficient and intelligent physical infrastructure, such as solid waste management system, energy and water-supply system, high-speed broadband system, housing stock, and urban mobility. For example, (i) Solid waste management system refers to generate, prevent, characterize, monitor, handle, reuse and disposition of solid wastes; and (ii) Urban mobility focuses on quality of walking, cycling, and smart transportation system in cities.

3) Social Infrastructure: Involves diverse mechanisms to promote and develop human and social capital, and provide intelligent and straightforward connected infrastructure for addressing different social needs and services of citizens, including education, health-care, environment, and inclusive planning.

4) Economic Infrastructure: Refers to the basic facilities and services that help to promote the process of production and distribution of economic activities and develop proper infrastructure to generate employment opportunities and attract investments. Although, this type of activities may not directly produce goods and services, they usually have effect on external economies by persuading production in agriculture, industry and trade.

It is undeniable that the smart city concept can transform every part of today's societies. As a result, by evolving the smart cities and increasing the connectivity and communications prerequisites, it is essential to collect and interpret huge volume of information. The analysis of such information helps governments to understand how to intelligently react to critical situations. Storing, analyzing and processing of such an amount of data will trigger the necessity for information security at all phases. Fig. 3 illustrates the pillars infrastructure of the smart cities.

D. Smart City Applications

Smart city has been emerged as a new concept that provides plenty of applications to promote the cities and environments. This section makes an overview on the existing application of the smart city.

1) Smart Energy: As a fundamental application of the smart city is responsible for providing a liveable, affordable, climate-friendly, and engaging environment for the citizens. The objective of smart energy is to efficiently control the energy and resource consumption and increase the usage of renewable-energy sources on the basis of an integrated and resilient resource system, and insight-driven and pioneering approaches to strategic planning. Smart energy concept relies on the following key elements: (i) Resource system integration: indicates the physical and digital plans to control resource flows with the aim of regulating resource efficiency and optimizing energy level through city systems, (ii) Access to energy services: indicates all citizens must have capability to reach reliable, affordable and sustainable energy services, (iii) Resilience: refers to preserving the communities and economy of a city for a long-term and make the city flexible and resistant to any kind of changes, especially in climate, by following an effective plans for the functions of city systems, (iv) Energy efficiency: is recognized as a key factor of smart energy due to the scarcity of available natural resources, (v) Renewable energy: one of the important goal of smart cities is encouraging the big companies and organizations to use the green renewable energy resources to prevent further and unpredictable climate change, (vi) Active and engaged users: the effectiveness of smart energy strategies depends on engaging businesses, citizens and academia in participating in the operational running of the city and its services, and (vii) Sustainable economy: the smart energy systems would be sustainable if utilizing the provided services and energy could economically be feasible for the citizens [39].

2) Smart Building: Refers an effective way for measuring, monitoring, controlling, and optimizing operations and maintenance by exploiting progressive automation and integration. ICT plays an important role in the expansion and operation of smart building in which generating a real-time response to the ever-increasing stream of data relies on analytics and data management. In other words, the produced data by the sensors, monitors, and controllers of the smart building can be collected and analyzed in the real-time mode to keep everything under control. One of the main applications of smart building is to manage the energy equipment by automatically replying to both internal policies and external signals to reduce energy consumption and increase the energy reliability [40].

3) Smart Mobility: Offers an effective way to transport people and goods with the aim of achieving a smooth and sustainable society on the basis of optimizing the difference types of transportation services for the citizens, through coordination of diverse transportation modes of the cities. One way to achieve a smart mobility system for a city is to build a network for collecting, processing, and analyzing data from the transportation systems of the existing organizations. For example, Hitachi proposes an architecture to support smart mobility in a city, including the following layers: (i) Transportation user experience layer: to deliver various information about transportation services to citizens, (ii) Transportation services layer: that contains provided transportation services by organizations, (iii) Information collection layer: to gather the information about usage of services, (iv) Information management and control layer: that check the services to confirm the smoothness of provided services by organization, and (v) Transportation company coordination layer: that is responsible for optimizing the city's overall transportation system by analyzing the collected information from all companies [41].

4) Smart Infrastructure: Consists of intelligent and automated systems for a smart city to communicate with, control, manage, and integrate into diverse types of intelligent infrastructure, such as smart people, smart mobility, smart economy, and smart energy. The main objective of smart infrastructure is to ensure the optimal usage of resources and improving the performance. However, there are numerous challenges to cope with for implementing a smart infrastructure concept, especially in developing countries, such as: localization and lack of human skills, finance, and well-developed business models. Moreover, designing a smart infrastructure relies on taking the following key principles into account: (i) It is a people-centric approach in which we need to consider the requisite of citizens when developing a smart infrastructure, (ii) Resiliency and sustainability to prevent unpredictable internal and external shocks, (iii) Interoperable to be involved all necessary components and flexible to support the future modifications and enhancements, and (iv) Risk-mitigating and safe to ensure the privacy and security of citizens against hacking and illegal access [37].

5) Smart Governance: As one of the main components of smart city provides an efficient way to simplify and support better planning and decision making based on using ICT tools. It also helps to emerge an integrated smart city by linking the relevant public, private, civil and national organizations. The major roles of governance in the smart city are: (i) Provide an opportunity for citizens to contribute significantly to governance and reshaping city life, (ii) Expressing appropriate policies and strategies for achieving ground-breaking sociotechnical and socioeconomic aspects of life, (iii) Supporting human and social capital investment, and (iv) Involving technological, organizational, and policy novelty [42].

6) Smart Education: Has an undeniable effect on improving the physical performance of the cities and cultivating new generations for life in a complex world of the future. The advantages of smart education can be clearly perceived from different perspectives. On the one hand, from the building viewpoint, applying an intelligent system can help the educational centers to have a comprehensive control and management on their energy systems, security levels, communication, and transportation. On the other hand, the intelligent system of smart education can provide new facilities for students by engaging modern technologies or social media, such as virtual, online, and e-learning [43]. For example, Microsoft recently offered a target-based game, namely Minecraft, to cultivate the problem-solving skills of the pupils in a collaborative learning environment [44].

7) Smart Health-care: Indicates offering health services on the basis of context-aware network, and ICT infrastructure of smart cities. Smart Health-care is a revolutionary concept, which naturally has effects on many senses: (i) Society: promoting the health-care services can clearly help to create a healthier society in which the citizens focus more on appropriate nutrition and physical activity, and the patients can benefit from effective treatments with the minimum cost, (ii) Government: applying a smart health-care can significantly reduce the health-care cost for government, for example, by empowering the detection and prevention mechanism, and (iii) Research: adopting a smart health-care model in a society results in collecting a huge amount of data that can be used by researchers to perform experiments to acquire knowledge on different areas of human behavior, health-care, and engineering [15].

8) Smart Citizen: Is recognized as a fundamental prerequisite of smart city that causes creating a fully comprehensive, groundbreaking and sustainable city. The smart citizens usually apply smart and green solutions in daily activities, create novel services and products, discover new methods for sharing information, and actively participate in a decision-making process [45].

9) Smart Traffic: One of the biggest challenges of the big cities is to design an effective and smart traffic management system. The Federal Highway Administration reported that more than 25 percent of traffic congestion in such cities are created due to the enormous number of traffic incidents. Moreover, traffic congestion causes various issues such as wasting time, increasing pollution and safety concern, and affecting economic development and quality of life of citizens. Smart traffic concept is an effective way to tackle this fundamental issue by tacking a quick decision based on the collected data from sensors, mobile devices, license plate readers, and CCTV cameras. There are three main approaches to manage the traffic: (i) Being prepared for unknown changes

and restrictions by keeping the citizens informed through smart traffic lights and signs; (ii) Responding dynamically to unpredictable disasters and changes, such as accidents and bad weather conditions, by using Real-time traffic light management or routed around obstacles; and (ii) Modifying the urban planning on the basis of the collected data from the traffic rate and the rout infrastructure to decrease the traffic [46].

III. Security Requirements of Smart Cities

Over the last decades, ICTs have played an important role and become as an inseparable part of the modern life. For example, the researches [47], [48] recently show that about 15 billion devices have the capability to be connected to the Internet on 2015 and around 50 billion by 2020, which may modify the way we are working, playing, or even doing the daily chores. It also affects almost everything, range from personal lives, education, and health to national security. Therefore, the implementation and adoption of smart city programs have become an objective of the majority of governments to manage water, energy, health, transportation, waste, surveillance, and security.

Although the smart cities make the life easier and help us to manage and control different aspects of the environment, increasing the complexity, interdependencies, and connectivity makes the smart cities more vulnerable against security and privacy attacks. The restricted or lack of understanding of security challenges and requirements of smart city may lead to unsuitable and insecure implementation and execution of the smart city. In this section, we will discuss the indispensable requirements for a secure smart city, which have to be taken into account at the design stage. These security requirements have been found in the relevant studies about smart cities by using some keywords, such as security/ requirement/ smart city/ IoT/ big data/ cloud/ cloud of things/fog and edge.

A. Secure Communication

Network communication is known as an essential component of the smart city architectures to join different components of the smart city for collecting, sharing, and transferring data throughout the cities. Establishing a secure wire and wireless communication in smart cities depends on confidentiality, integrity, and non-repudiation as the important features of network security [49], [50]. One of the best ways to secure the smart cities communications is to develop lightweight cryptographic methods for encrypting and decrypting data and creating a shared secret key among various nodes. However, applying such security algorithm to different network components is a crucial challenge in smart cities, due to the heterogeneity of the devices that are connected to the network and used to collect or share data. The next challenge for making the communication secure is to design an effective distributed key management system (e.g., [51] and [52]) for providing secure communication, due to the geographical distribution of smart cities. The key management center usually generates the primary keys (public and private key) with proper length and lifetime for all components to meet the security objectives and at the same time not drain the embedded system's resources.

Recently, Rambus [53] proposed a CryptoManager IoT Device Management system for identifying and authenticating the IoT devices on the basis of pre-provisioned unique device keys. This management system also help IoT devices to create a secure communication channel to other devises and services. Once an IoT devices connected to the network (e.g., Internet), the device has to be seamlessly authenticated by CryptoManager IoT Device Management. The system also generates appropriate security credentials for the IoT device. However, this crypto system is unable to support a wide range of IoT devices.

B. Secure Booting

Viruses, worms, and other malware have the capability to overwhelm the systems through the boot sectors where in the such viruses are located as an executable code and are able to be distributed to the other systems through the Internet connection or upon booting the other system using infected disks. Pre-boot malware is also able to be executed before the system is controlled by using an Operating System (OS) kernel and then hidden out in ways that are impossible for the OS and virus scanners to detect the malware.

Indeed, secure boot is designed as an additional layer to protect the system against the pre-boot process. Secure booting is a technology for helping the system firmware to check the existence of a cryptographic signature for the system boot loader. Since the cryptographic key of the signature is stored in the firmware database, it is difficult for the malware creator to sign the malware if the key is controlled by the authorized user. As a result, the firmware refuses to execute the program, which contains the unsigned malware. The firmware can also verify a malware on the basis of a cryptographically generated digital signature in the next-stage boot loader, kernel, and user space. In other words, the secure boot is a require technology for smart city devices that guarantees the integrity and the authenticity of the software packages and avoids the execution of unsigned code [54].

Although the existence of secure booting is vital for the IoT devices to protect the authentication and integrity of the software on such devices on the basis of cryptographic hash algorithms, the majority of boot securing techniques are inapplicable for IoT devices. This is because Such devices are suffering from low processing resources. Therefore, it is essential to design an efficient boot securing for IoT devices by using ultra-low power consumption hash functions [55]. NH and WH universal hash function [56] are examples of hash functions for ultra-low power consumption devices [56], [57].

C. Security Monitoring, Analysis, and Response

Monitoring strategy is a indispensable requisite for all systems to control the surrounding environment and detect the active attacks and anonymous behavior. The automated response systems must have access to adequate information about attacks and automatic detection of suspicious behavior,

due to the scalability of IoT systems in terms of the number of devices and the amount of information being processed. The system may consider different strategies for responding to attacks and doubtful behavior: (i) Elimination strategy to temporarily isolate, quarantine, or completely remove such parts of IoT devices, and (ii) Response strategy in which a formal incident response process is considered to cope with vulnerabilities that are detected upon the systems have been put into service.

Indeed, the smart city systems require appropriate strategies to disclosure the potential vulnerabilities with the aim of migrating, modifying, and updating all affected parties in a timely manner. This is because the IoT devices, which are in charge of collecting and transferring data, are vulnerable against a wide variety of attack forms. For example, injection of fake, erroneous, or erratic sensor data are the forms of attacks into the IoT systems, which are able to redirect decisions of the automated system to behave in attackers desired manner (e.g., to force the automated response system to take the exception strategy) [58].

For example, Cisco designed a security monitoring, analysis, and response system to: identify the network threats on the basis of learning the network topology and configuration; providing recommendations for mitigating threats by identifying the source of threats, and incident management. However, this mechanism is only applicable for Cisco network equipment [59].

D. System, Application, and Solution Lifecycle Management

As it is clear, smart cities rely on the IoT devices to collect, analyze, and get in touch with the citizens. Therefore, increasing the demand for IoT solutions results in developing the application without compromising security and reducing performance of the system. However, the enterprise customers expect the developers to anticipate the necessity of systems in the near future. Moreover, the necessary actions and plan for the entire life-cycle of IoT devices and applications have to be predicted at different design stages of smart cities. Lifecycle management of the IoT systems needs a high level of complexity and has a direct relation with identity management, device management, and development of application and software by modifying the management of deployed and in-service systems. The necessity to connect any types of devices, even those that are not designed for connectivity, forces the IoT systems developers to make sure about the security of such connections. As a result, the developers have to consider protective measures at all levels device, network, and cloud. Moreover, the developers have to validate the code, key material, and even physical components of such systems in all stage of development and installation. After securely connecting, the IoT devices must have capability to securely upgrade their distinct components for overcoming the vulnerabilities, achieving the functional enhancements over the lifetime of the system, and protecting the privacy and security of data. Finally, it requires to address the challenge of integrating the IoT devices with other city systems that can aggregate, analyze, and act after collecting the data from devices, to make a bridge between operational technology and information technology systems [58], [60].

Consider [61] as an example in which a new data management lifecycle model, namely Smart City Comprehensive Data Life Cycle (SCC-DLC), is proposed for smart cities based on fog and cloud resource management architecture. The SCC-DLC model is able to efficiently manage and organize huge volume of data, which are collected from diverse information resources, during data acquisition, data processing, and data storage of smart cities. The main contribution of this work is to add a new layer including several fog nodes for the smart city architecture with the aim of increasing the computation and storage capacity as well as reducing the network traffic and communication latencies. Although reducing the data transmission latency may have a positive effect on security risk and communication failure, the security and privacy of data has not been measured in this architecture.

E. Updating and Patching

Updating and patching are the important necessities of the IoT devices to work properly and be secure against the most-recent malicious attacks. This is because by developing the technology, we are facing the new and complex security attacks that may not be overcome unless receiving the software updates. Moreover, it allows the enterprises to identify the vulnerabilities and address them efficiently. The devices should also have an aptitude for authenticating the received patches through their operators and service providers [62]. However, the authentication process must not have any side effect on the functional safety of an IoT device and its interconnection with other devices, especially when they are in charge of performing vital operations and need security patches to be protected against vulnerabilities. It is important to mention that the software updates, and the security patches should be provided in a compressed package to be downloadable through the limited bandwidth and diminish the probability of compromising functional safety [63].

Despite the fact that patching and updating are the effective way to avoid cyber-attacks, upgrading or patching is one the biggest challenges for some of the IoT devices. For example, it is impossible to install and run any antivirus as a third party endpoint security solution on IoT devices with medical applications. There are two reasons for supporting this claim. On the one hand, the majority of medical device manufacturers suffer from lack of experience for supporting dynamic patch update. As a result, such devices only rely on secure communication channel for transferring the collected data. On the other hand, updating the medical devices is very rigorous and time-consuming process because of the existence restrictions in the food and drug administration [64].

F. Authentication, Identification, and Access Control

The power of IoT systems and devices are highly dependent on sharing data and combining different inputs as well as processing and creating additional values. As a result, it is essential to control and manage the generated data by other IoT devices, while preventing the use of data in

TABLE III
COMPARISON OF SECURITY REQUIREMENTS FOR SMART CITIES

Requirements	Method	Challenge
Secure Communication	Lightweight cryptographic Methods	Heterogeneity of Network components and devices
	Distributed key management system [51], [52]	Geographical distribution of smart cities; Draining the embedded system's resources
Secure Booting	Cryptographic boot system	Adoption to heterogeneous IoT devices
Security Monitoring, Analysis, and Response	Cisco Security Monitoring, Analysis, and Response System (MARS) [59]	Only applicable for Cisco network equipment
System, Application, and Solution Lifecycle Management	Smart City Comprehensive Data Life Cycle model [61]	Lack of security and privacy measurement
Updating and Patching	Microsoft and Linux patch updating	Authenticating the update package may reduce the IoT device functionalities; May not be applicable for old IoT devices
Authentication, Identification, and Access Control	IBE [68], ABE [69], RBAC [70]	Are only applicable for cloud-based IoT systems; May incur high computation cost on IoT devices.
Data and Application Protection	Securing IoT devices, Access permission monitoring, Securing communication links using cryptographic methods	Lack of a comprehensive framework to provide security and privacy of all layers of smart cities simultaneously.

unauthorized or undesired ways [65], [66]. The authentication of IoT systems by constructing secure communication between the included things, is a crucial perquisite for smart cities to manage the access control of the legitimated citizens in an authorized manner and prevent unauthorized users to access resources [67]. In order to construct a solid communication, different authentication and access control protocols, such as Identity-Based Encryption (IBE) [68], Attribute-Based Encryption (ABE) [69], and Role-Based Access Control (RBAC) [70], have been designed to protect the security and privacy of data especially in cloud-based smart cities. This is because the citizens' information is collected and outsourced to the distributed data storages, which are controlled and managed by unauthorized Cloud Service Provider (CSPs). These schemes enable the smart city applications to securely handle the authorized users and revoke their permission rights. For example, the objective of attribute-based access control is to render the existing attributes of the data owner, users, or the other IoT devices to implement the data access control [71].

G. Data and Application Protection

Smart cities rely on the different components of the sensing layer architecture, which are responsible for collecting the huge volume of large-scale data from different resources and storing them in the local or remote storages (e.g., cloud computing). Considering with the diversity of collected data and the security level from personal to public information, designing a flexible and an efficient data security and privacy method play a vital role in smart cites. In other words, the smart cities have to leverage multiple methods simultaneously for identifying the system vulnerabilities and providing different levels of data protection against the internal and external threats in all layers of architecture of smart cities. The first step to protect the data security in smart cities is to make the IoT devices secure by using the existing techniques. For example, preserving the privacy of smartphone applications depends on: (i) Securing the unique identifiers (e.g., UDID (Unique Device Identifier), IMEI (International Mobile Station Equipment Identity), and MEID (Mobile Equipment Identifier)) of smartphones by preventing the application from sharing them, and (ii) Monitoring on the access permissions that are issued for application to gain access to private data in smartphones [72]. Then, the communication links have to be protected by using the existing cryptographic algorithms and key management methods to securely transfer data among the components of smart cities and provide end-to-end and point-to-point communications protection. Finally, the different format of data stored in the databases and even whole disk level have to be encrypted to prevent data leakage and improper usage [58].

Table III compares the general requirements for securing smart cities on the basis of method and challenge attributes. The method attribute indicates the general solutions to meet the security requirement of smart cities and the challenge attribute represents the encountering issues and challenges for adopting the suggested methods to smart cities.

IV. SECURITY ISSUES AND CHALLENGES OF SMART CITIES

Smart cities consist of complex, networked assemblages of digital technologies, ICT infrastructure, and IoT devices for handling different services and system throughout the cities and optimizing the resource consumption. Since the IoT devices of smart cities require to be interconnected through different types of networks, they expose to the huge number of security risks and there are more potential entry points for attackers across networks. In this section, we first explain the effect of cybersecurity threats on the security of smart cities. We then classify the existing security issues and challenges on the basis of the different types of smart cities into two groups: IoT-based and cloud-based smart city challenges. These security issues and challenges have been retrieved from the relevant studies about smart cities by using the following keywords: security/ issue/ challenge/ smart city/ cybersecurity attack/ IoT/ big data/ cloud/ cloud of things/fog and edge.

A. Cybersecurity Attacks on Smart Cities

Smart cities consist of complex, networked assemblages of digital technologies, ICT infrastructure, and IoT devices for handling different services and system throughout the cities and optimizing the resource consumption. Since the IoT devices of Smart cities consist of thousands or millions of interconnected IoT devices, which are responsible for collecting and transferring data. As a result, the malevolent intruders are able to leverage the structure of smart cities to create and deploy self-propagating malware, which can be disseminated across multiple connected networks. The attackers can easily gain access to sensitive information, such as healthcare financial and bank credentials of users. They are also able to perform different types of cybersecurity attacks with the aim of destroying: (i) Confidentiality to extract the information and monitor the system activities, for example, the illegal data collection through eavesdropping or analyzing message traffic; (ii) Integrity to modify the information and change the system setting, for instance unauthorized access to sensitive information, (iii) Availability to make the system close and unavailable for authorized users, for example Distributed Denial-of-Service (DDoS) is a type of availability attack; and (iv) Authentication is a major security threat to IoT devices in which an unauthorized user has capability to send, receive and replay most types of messages [14].

Over the last decade, Distributed Denial-of-Service (DDoS) attacks have been emerged as one of the major security threads to public Web servers, in which cloud infrastructure providers are responsible for providing services to users. DDOS attacks also have disastrous influence on different aspects of smart cities. For example, adversaries are able to leverage the botnet to launch DDoS attacks to traffic and surveillance cameras as the eyes of smart cities [73]. Moreover, smart city application servers and cloud infrastructure are commonly faced with application layer DDoS attacks as catastrophic challenges, in which a huge volume of traffic is generated on the Web servers to bring down the network services and disrupt the services [74]–[76]. Since the smart cities usually require data centers as hosts of a variety of Web-based application servers, they are commonly suffer from such attacks. As a result, proposing a defense model against application layer DDoS is essential for smart cities with the aim of protecting smart services and applications. However, the distinct and distributed nature of smart cities in terms of volume, velocity, and variety of network traffic makes it very difficult to propose an effective method to mitigate such attacks. There are also some other challenges, such as networks heterogeneity, high availability and scalability, and dynamic security policies of smart cites have to be accounted for designing such mitigation model. To address these issues, Bawany and Shamsi [77] proposed an efficient framework to detect and mitigate the flash crowd application layer DDOS attack in smart cities, where the legitimated connections on a server or website are suddenly increasing simultaneously or within a short period. The main idea behind this method is to use a master city controller component to effectively analyze and filter the malicious traffic from legitimate traffic flows on the basis of Software Defined Networking (SDN) concept.

Side-channel is a type of physical attack for smart cities in which the attacker threatens the security of most cryptographic IoT devices by using physical information leakages such as timing information and power consumption. The next type of security attacks in smart cities is brute force in which the adversary is able to exploit the existing vulnerability of the network to breach a network perimeter and gain access to encrypted data or key.

Table IV compares some of the existing intentional attacks and shows their side effects on the smart cities.

We classified the security issues and challenges on the basis of the different types of smart cities into two groups, such as IoT-based and cloud-based smart city challenges, as follows.

B. IoT-Based Smart City Challenges

The first group of smart cities, which is constructed on the base of IoT technology, is known as an IoT-based smart cities [65]. Upon collecting data by using the deployed connected IoT devices and smart objects, the data will be stored in the local temporary storage to be accessible by the data analytical layer to perform real-time and batch processing. There are various security issues and challenges that threaten IoT-based smart cities, which have been classified and evaluated based on the architecture of smart cities, and discussed in the rest of this section.

1) Connected Devices and Smart Objects Issues: The connected devices play an important role in different layers of smart cities for collecting, transferring, temporary storing, and even analyzing the data. There is an enormous amount of security issues against the smart devices, which we briefly elaborate some of the related issued to smart cities, as follows.

a) Data over-collection with dynamic active cycle: Smartphones are known as inseparable parts of our life, which provide different services for users, such as health-care, environment mate and monitoring, financial works, and electronic ID. The connected devices have the capability to be used as a mediator storage or a fog node to perform a small computation in the network. These diverse applications of smart devices make them more vulnerable to some security attacks, although such devices may be active or waste in any situations [86]. As a result, it is essential to develop a novel security method to cope with these challenges [87].

Recently, the huge number of applications have been proposed by different enterprises to provide various benefits for end users. However, the majority of these devices usually need to gain access to private information of users and transfer the collected data to unauthorized third parties. This process may threaten the security and privacy of the users by revealing their information to the third parties. Moreover, these application usually collect more data than the necessities of original functions, while in permission scope, which is known as data over-collection. Therefore, it is essential to design the effective solutions to cope with the data over-collection issue in smart cities [79].

b) Heterogeneous interaction and the requirement of the lightweight cryptographic algorithm: The connected devices and smart objects usually interact in heterogeneous

TABLE IV
CYBERSECURITY THREATS AND THEIR EFFECTS ON SMART CITIES

Attack	Key Features	Compromising			
		Conf.	Integ.	Avail.	Auth.
Eavesdropping [14]	• Capturing network traffic and listening to communications between two or more parties. • Disclosing details regarding the configuration of the network.	✓	✓	✓	
Cross-Site Request Forgery (CSRF) [78]	Forcing an end user to execute unwanted actions on an attacker web application to perform state-changing requests, such as transferring funds and compromise the whole web application.				✓
SQL Injection Attack [79]	Inserting a SQL query via the input data from the client to the application to read or modify data, or execute administration operations on the database.	✓	✓		✓
Cross Site Scripting (XSS) [80]	Injecting client-side scripts into web pages by attacker to evade access controls such as the same-origin policy.	✓			✓
Side-Channel Attack [81]	Exploiting the available information (e.g., plaintext, cyphertext, or timing information) to find a user's key and retrieve data from a encrypted device.	✓			✓
Distributed Denial of Service (DDoS) [79]	• Overloading a targeted resource by consuming available bandwidth. • Overwhelming targeted resources by using protocol flaws. • Overloading application services or databases with a high volume of application calls.			✓	
Brute-Force Attack [82]	Using many passwords or pass phrases to eventually guess the password and hack into network.	✓			✓
Replay Attack [83]	Eavesdropping a stream of messages between two parties and fraudulently retransmit it to one party to perform unauthorized operation, such as false identification and authentication.				✓
Session Hijacking [84]	Exploiting a valid session key or stealing a magic cookie of an authorized user to acquiring unauthorized access to information or services				✓
Virtual Machine (VM) Escape [85]	Breaking out a virtual machines (VM) and interacting directly with the hypervisor to obtain access to the host operating system and other VMs running on that host.	✓			✓
Unauthorized Access [71]	Including unauthorized network connection, data leaks, browsing files, obtaining private data, controlling field components and using resources	✓	✓		

environments due to the diversity of manufacturers and enterprises for designing such devices under different standards, protocols, and technical necessities. As a result, it is very difficult to propose an effective method that can meet the security requirements, homogeneity, and interoperability criteria of all smart city devices. This situation becomes worse, when we are encountering the device network's points of connection that uses the external networks (e.g., the Internet and public Wi-Fi). This is because the end-to-end communication suffers from the connection that frequently requires gateways or proxies [88]. On the other hand, the majority of connected devices have the low level of power and computation resources. Therefore, IEEE 802.15.4 has been developed to address the connectivity issue of connected devices through Low-Rate Wireless Personal Area Networks (LR-WPAN), which needs low power consumption, low deployment cost, less complexity, and short-range communication [89]. However, this IEEE standard causes several security attacks such as DoS, which have adverse effect on key exchange protocol of connected devices, due to fragmenting large packets of security protocol [90].

To sum up, it is problematic to propose an efficient, secured, and lightweight cryptographic algorithm (e.g., key management) for providing a secure end-to-end communication channel, due to the heterogeneity and power restriction of IoT devices and smart objects [91].

2) Data Sensing, Storing, and Transition Issues: The IoT devices throughout the smart cities are responsible to collect sensitive data and transfer them into databases or cloud storage throughout wire and wireless links. However, there are some security issues that may impact on sensing and storing process in smart cities, as follows.

a) Secure storage and transaction logging: Smart cities encounter with big data storages as a critical challenge in which the huge volume of collected data needs to be stored in large-scale databases. Auto- tiering storage has been provided recently as an effective way to alleviate this issue where in different levels of storage are automatically assigned for items on the basis of policies established by the organization. However, because of the presence of unverified storage services and mismatched security policies, there are several vulnerabilities that threaten the security of auto-tiering databases: (i) The auto-tiering databases automatically reallocate the data based on the rate of the access requests with the range of rarely accessed to critical information. As a result, less security has been characteristically attached to such data, which is seldom requested and located at a lower tier of database. (ii) In addition to preserving the security of the stored data in such databases, their transaction logs that contain a list of the database activities have to also be secured with the aim of protecting the stored data and logs information. (iii) The auto-tiering databases suffer from collusion attack in which the service providers are able to access more information that has been determined for them because the keys and access codes are exchanged by them. (iv) The rollback attack can also break the security of such databases by replacing the outdated dataset to the latest version [92].

b) Data validation and filtering: The effectiveness of smart cities relies on collecting the useful data at the exact

time to perform the real-time data analysis. However, due to the extensiveness of data sources and the huge volume of data, performing analysis on such an amount of data is a challenging task. On the other hand, it is very difficult for smart city applications to verify and validate the collected data, which has a direct effect on the accuracy of the output of such applications. In other words, determining the data validation is a major challenge in the smart cities, which depends on the different factors, such as data source, data type, and connection link. As a result, the data collection layer of the smart city architecture requires an applicable way to identify the malicious data sources, filter the unreliable data, and detect the possible attackers (e.g., ID clone attack, and Sybil attack) who feed the fake data to the system by spoofing multiple IDs.

3) Data Processing and Aggregation Issues: The data processing is one of the essential layers of smart city architectures, which is responsible for carrying out the batch and real-time analytics on large-scale of data. However, there are some security issues that threaten the different components of this layer and have a direct effect on the its performance, as follows.

a) Transmission of critical data for real-time analytic: Performing real-time analytic on sensitive data is one of the main applications of smart cities. Data processing is a complicated and real time-demand process, especially when the security of data needs to be preserved by using a powerful cryptographic algorithm. In other words, data encryption and decryption methods make the data processing extremely difficult and time-consuming. This is because the processing methods encounter a huge volume of data in different formats, and communication protocols [93]. On the other hand, since encrypting and decrypting data commonly have a side effect on the performance of the real-time data analytic procedures, the majority of smart city platforms prefer to increase the rate of real-time data analytic rather than using effective cryptographic algorithms to ensure the security of data analytic through the smart city architecture.

b) Data provenance and verification: The smart cities have a wide variety of resources, including millions of citizens and end-user machines in enterprise settings, which usually generate huge volume of data result in increasing the complexity of the provenance. The data object commonly consists of the provenance information as a metadata, which provides enough information about the object's creation. In other words, the provenance metadata of smart city applications contains the provenance for the infrastructure of the smart city, which is presented as a meta-metadata. As a result, the complexity of provenance metadata is dramatically increasing by developing the area progresses because of generating large provenance graphs from provenance-enabled big data applications. Moreover, the computation cost of analyzing such complex graphs in this size is highly resource-intensive. The major security threat to such area is about malfunctioning infrastructure, and attacking on infrastructure from inside or outside of the organization with the aim of altering the data integrity of big data applications in smart cities. Moreover, to effectively verify the data sources through any audit and detection method, it is essential to preserve the security of provenance metadata [92].

C. Cloud-Based Smart City Challenges

The IoT-based smart cities provide the enormous number of applications and facilities, ranging from smart health-care to smart governance, for citizens. However, the connected devices as the fundamental of IoT-based architecture commonly suffer from some restrictions, such as the computation, energy, and storage resources that can be efficiently overcome and supported by integrating the IoT and cloud computing [94]. Albeit cloud-based smart cities are able to cope with the shortcoming of IoT-based smart cities and connected devices by outsourcing the information and computation to the CSPs and delegating the management of data to the remote servers, cloud-based smart cities are still vulnerable to the majority security of IoT-based smart cities (presented in Section IV-B). Moreover, such integration results in emerging some new security challenges, as follows.

a) Data and computation outsourcing: Cloud computing provides an effective way to store the huge amount of collected data and perform the computation with minimum overhead on connected devices in the smart cities. However, by outsourcing the data in the remote servers, the physical control over the data is taken away and the management of data is delegated to an untrusted CSP. The cloud is inherently neither secure nor reliable from the view point of the clients and it raises new challenges to the integrity of outsourced data in cloud storage. As a result, devising a proper audit service, which can remotely check the integrity of outsourced data in the cloud-based smart cities is deemed as a crucial need [95].

b) Physical location of data: Integrating cloud computing and IoT applications helps to efficiently manage and store the huge amount of data in the smart cities. However, the cloud service providers are not completely honest and may store the data in different level of cloud storage and try to conceal it from end users' view point. As a result, lack of knowledge about the physical location of data in cloud storage may influence on the data security and quality of services [83].

c) Lack of knowledge about service level agreements (SLAs): Assuring the predictable service levels in cloud-based smart cities relies on establishing a tailor-made SLA, which is a contract between the cloud customers and CSPs as two parties of services with the aim of ensuring the commitment of SLAs and interaction experience of the consumers by CSPs [96]. The SLAs contain critical information and different specification about the services, security and risk management, priorities and responsibilities, pricing, and performance of provides services to the customers. As a result, the SLA has a critical role in the cloud-based smart cities to provide a trust level among the existing components. However, the majority of IoT devices suffer from lack of knowledge about the existing SLA [97].

d) Multitenancy: The concept of multitenancy is known as a key difference between cloud computing and locally managed computing in which many tenants share the resources and information and delegate the management of them to the CSP. In other words, the service providers have the capability to provide an efficient, scalable, and share environment for computing tenants' tasks and storing their information in the same database and may even share the same tables. However,

the multitenancy may also lead to raise some security concerns regarding the information leakage and data breach, as follows: (i) Cloud computing provides a virtualized infrastructure for different customers to take the co-residency of machines in a privileged position relative to one another, which may increase the risk of unauthorized connection monitoring, malware propagation, unmonitored application login attempts, and several man in the middle attacks. (ii) Since the important information of different tenants is stored in a database as rows in tables distinguishing by customer ID, there is a possibility to put such information at risk of theft and misuse by misconfiguring an application code or an error in an access control list. As a result, cloud-based smart cities require multitenancy protection techniques to prevent data loss, misuse, or privacy violation [98].

e) Data retention: Cloud-based smart cities provide a powerful infrastructure for citizens to outsource their critical information to the cloud storages for optimizing the storage and maintenance cost. The CSP usually keeps multiple backups and copies of the outsourced data in different forms such as index structures, which may not be directly connected to the cloud. Therefore, there is not any guarantee that when citizens ask to delete the outsourced data, the CSP removes all copies of data within a timescale, which is in line with their own deletion schedule [99], [100].

Table V compares the security challenges of the smart cities on the basis of different attributes. Type of challenge is the first attribute to classify the security challenges based on the architecture of smart cities into IoT-based and Cloud-based smart cities. Security challenge is the next attribute that lists the existing security issues. We finally presented a brief expiation of such challenges, including specification, security requirement, and definition, to highlight the difference of challenges in description attribute.

V. Privacy Concerns of Smart Cities

Data privacy is known as a crucial challenge and concern in smart cities, which relies on collecting, storing, sharing, and analyzing the huge volume large-scale sensitive information by IoT devices. In other words, the effectiveness of smart cities depends on successfully employing big data application as an inseparable part of such cities. This is because the IoT devices in smart cities usually capture huge volume of data for storing and further analysis [101]. On the one hand, integrating these two concepts requires to tackle several challenges, which may be related to either the nature of smart city needs or big data features, as follows: (i) Bach processing: is an effective way to process and analyze a huge volume of data that is collected over a period of time and stored in NoSQL databases. Batch processing needs a distinct program (e.g., Hadoop's MapReduce [102] or Hama's Bulk Synchronous Processing framework [103]) for input, process and output. (ii) Real time processing: includes a continuous input, analysis, and output of data flows with high performance in which the processing of data has to be in a small period of time or near real time. (iii) Big data management: offers a confident way for utilizing the accumulated data in smart city applications by developing architectures, policies, and procedures to accurately manage the data. (iv) Network infrastructure: It is commonly impossible to create a smart city without existing powerful and comprehensive network infrastructures, which are in charge of delivering data among different components and layers of smart cities through wired or wireless connections. The network infrastructure also plays an important role in the decision-making process in the real-time big-data applications. (v) Complex and sophisticated algorithms: are responsible to effectively process high volumes of data with large variety in heterogeneous and dynamic environment where the use of traditional algorithms is impossible [104], [105].

On the other hand, emerging big data scenarios in smart cities for collecting, storing, sharing, and analyzing the personal and sensitive information by IoT devices have caused privacy concerns. Due to the wide-range applications of smart cities, the privacy issues may threaten various resources, such as healthcare records, location-based service and geolocation, residence and geographic records, Web surfing behavior, and financial institutions and transactions. For instance, a car-based telematics system usually collects data that is extremely treasured for insurance companies to increase someone,s premium or even reject a new contract [106]. Consequently, the majority of citizens prefer not to allow IoT devices to collect the sensitive data, which may results in violating the data privacy by revealing the sensitive data to the third party. In other words, to acquire the maximum benefit from collecting and processing data in smart cities, it is essential to consider security and privacy as important requirements in all layers of the smart city architecture [107]. This is because some thresholds must be taken into account: (i) making commercial decisions with confidence highly depends on preserving the confidentiality and integrity of the data, (ii) controlling a physical environment in a safe and reliable way requires preserving the integrity and availability of the data, and (iii) sustaining and establishing public confidence is necessary for those who analyze and process the data for providing an efficient decision making and service delivery process [104], [108].

We have retrieved the privacy issues of smart cities by leveraging some keywords, such as Privacy/IoT/ cloud/ cloud of things/data privacy/ and smart cities. Generally, preserving data privacy in smart cities relies on meeting the following requirements.

A. Acquiring User Consent

The IoT devices in smart cities are responsible to collection data from different resources, which may be sensitive for data owners. However, collecting sensitive data without attaining user permission may violate the data privacy in smart cities. Requesting user permission in an effective and efficient way has been a main privacy issue in IoT-based devices. This is because the majority of users are suffer from time restrictions or inadequate technical knowledge to involve in the process [104].

B. Data Access Control and Customization

The collected data in smart cities may be stored locally or outsourced to the cloud computing. The data owners are

TABLE V
COMPARISON OF SECURITY CHALLENGES FOR SMART CITIES

Type of Challenge	Security Challenge		Description
IoT-based	Connected Devices & Smart Objects	Data Over-Collection with Dynamic Active Cycle	The majority applications designed for IoT devices require to gain access to private information of users and transfer the collected data to unauthorized third parties.
		Heterogeneous Lightweight Cryptographic Algorithm	Due to homogeneity, interoperability, and resource constrain of IoT devices, It is difficult to propose an efficient, secured, and lightweight cryptographic algorithm for providing a secure end-to-end communication.
	Data Sensing, Data Storing, & Data Transition	Secure Storage and Transaction Logging	Using Auto-tiering storage for securely storing huge volume of data is a critical challenges for smart cities, due to the lack of verified storage services and security policies.
		Data Validation and Filtering	Identifying the untrusted and malicious data resources, filtering unreliable data, and detecting intrusions in data collection layer is a critical issue of smart cities.
	Data Processing & Aggregation Issues	Transmission of Critical Data for Real-time Analytic	Although it is essential to protect the real-time data analysis by leveraging cryptographic algorithm, it directly reduces the effectiveness of such analytic algorithms.
		Data Provenance and Verification	Malfunctioning infrastructure, and attacking on infrastructure from inside or outside of the organization may threaten the integrity of big data applications in smart cities.
Cloud-based	Data Computation and Outsourcing		Designing an appropriate data auditing method to preserve the integrity of outsourced data is challenging due to the huge volume of collected data.
	Physical Location of Data		To ensure the security and quality of data, it is essential to provide knowledge about the physical location of data in cloud storage.
	Lack of Knowledge about SLA		Although SLA includes critical information about the services, security and risk management, priorities and responsibilities, pricing, and performance of provides services to the customers, the majority of IoT devices suffer from lack of knowledge about SLA.
	Multitenancy		The cloud-based smart cities need an effective multitenancy protection techniques to prevent data loss, misuse, privacy violation, malware propagation, unmonitored application login attempts, and man in the middle attack.
	Data retention		Removing data from remote data storage is challenging due to the existence of different copies of outsourced data in cloud-based smart cities.

always looking for having the full control on the collected data when allows them to delete, modify, or change the location of data. Unfortunately, the existing solutions are unable to provide full access control for users. The smart city users may also require to construct and customize their smart environment by selecting different hardware devices and software components. Furthermore, the users must have capability to grant and revoke access privileges to other users and service providers. Although services providers need to access some types of data to provide certain types of services, service providers have to fairly treat consumers. Disabling some features to a group of users and changing the subscription fees are examples of unfair service providers [105], [109].

C. Transparency and Reliability

Batch and real time data processing provide an opportunity for smart cities to offer a different number of functionalities for users. To achieve this goal, service providers requires to access certain types of collected data by IoT devices form variety resources. However, the service providers may be able to leverage the raw data with the aim of derive more information about the data owners without taking their permissions, which is against transparency [104], [110].

D. Anonymity

Collecting data through IoT devices and transferring data by using network communication provides a way for service providers to track back the communication paths and the user location (e.g., by leveraging the MAC address). Designing an efficient end-to-end anonymity method to protect user privacy on the basis of concealing data communication paths is still a critical challenge in smart cities because of the large number of IoT devices (e.g., sensors) for data collection. Although, a group of research recently focused on improving the privacy of users on the Internet by proposing Tor [111], we still need

a framework to ensure anonymity at all layers of smart cities (e.g., data collection, storage, and data analysis layers).

In the rest of this section, we review the privacy issues in data collection, storage, and analysis layers of smart cities.

1) Privacy in Data Sensing and Storage: Data sensing is known as a fundamental layer of the smart city architecture in which the IoT devices are used to collect the different type of resources and transfer them to the existing databases. The collected data, which may contain private information about a person, event, or thing), are vulnerable to numerous privacy and security attacks result in privacy leakage and information inferring. It is commonly impossible to protect the privacy of the citizens' data without informing them about the types of data that have to be collected and the main purpose of collecting such data [97]. There are some useful methods, such as data encryption, anonymity, and access control that ate used to preserve the security and privacy of data during data sensing phase. However, it is still possible to unconsciously disclose to untrusted third part. For example, the geographical location, lifestyle, and other private information of residents may be captured by using surveillance cameras, which initially intended to monitor criminal behaviors throughout the cities. Additionally, designing an effective method for protecting the security and privacy of data collection phase against inside and outside attackers in smart cities arise from a new complex challenge due to high granularity, large scalability, and diversity of data.

Although, integrating IoT devices with cloud computing addresses the storage and computational issues of smart city applications, outsourcing data to unauthorized cloud service providers imposes more privacy issues on citizens due to lacking of physical control over the data [83], [91]. As a result, it is impossible to protect the privacy of outsourced data by using the traditional cryptographic algorithms. Moreover, applying the complex security methods to protect the data security and privacy is not applicable for most of IoT devices with lifetime and computation restrictions. On the other hand, the existing cloud computing infrastructures suffer from the lack of privacy protection associated with the collecting and tracking of personal and sensitive data. Therefore, it requires to redesign cloud middleware for achieving an inherent privacy protection goals [112].

Data breach poses crucial threats to the privacy of outsourced data in cloud storage wherein an individual's name plus a medical record and/or a financial record or debit card is potentially put at risk. Data breach usually occurs in different enterprises for a reason of malicious or criminal attack, system glitch, or human error. Ponemon Institute under the sponsorship of IBM has issued an annual report about the 2016 cost of the data breach from more than 383 companies in the 12 countries, such as Arabian region (United Arab Emirates and Saudi Arabia), Australia, Brazil, Canada, France, Germany, India, Italy, Japan, United Kingdom, United States, and for the first time, South Africa. The research shows that the average cost of losing or stilling each record containing sensitive and confidential information reaches $158 in this year. The U.S. organizations experienced the highest total average cost of the data breach at more than $7.01 million, followed by Germany at $5.01 million. In sharp contrast, South African and Indian companies experienced the lowest total average cost at $1.87 million and $1.6 million, respectively. Moreover, to resolve a malicious or criminal attack, the U.S. and Canadian companies had to spend more than $236 and $230 per record, respectively [113]. As a result, it is essential to determine an effective method to overcome the data breach issue in the smart cities.

To sum up, the smart cities need to use the different form of privacy preserving techniques, including identity privacy to protect personal and confidential data; territorial privacy to preserve personal space, objects, and property; communications privacy to defend against the surveillance of conversations and correspondence, locational and movement privacy to protect against the tracking of spatial behavior and geographical location of things; and transaction privacy to protect against monitoring of searches, online purchases, and other exchanges.

2) Preserve the Privacy in Data Mining and Analytics: Although the big data nature of smart cities causes to develop the marketing rate and increase state and corporate control, it makes them vulnerable against invasions of privacy issues [114]. The citizens' data are usually accessed by different companies and contractors, government agencies, and business partners for different purposes. For example, there are an enormous number of companies that are using data analytic methods as an effective way to offer an unexpectedly complete picture and identify the potential new customers, but it may disclose the important information of individuals. Therefore, such companies are commonly responsible for ensuring the privacy of citizens by providing appropriate policies. A naive solution to protect the privacy issues of data analytic process is to leverage data anonymization techniques. However, these methods are inapplicable to the smart cities, because there are some data that can be used as an association with identification purposes [92].

The next important privacy challenge in smart cities is to perform data analytic algorithm on encrypted data. Preserving the privacy of collected data during data sensing and analyzing process is essential for smart cities in which an effective data encrypt must be used before sending the data to the analytic layer. However, such encryptions make the data analytic process very difficult, time consuming, and unsuitable for online data analytic process. On the other hand, decrypting the data threatens the privacy and incurs high computation overhead on the data analyzer.

VI. Security Solutions and Architectures for Smart Cities

Providing security and privacy for smart cities is a challenging task because these cities require to collect a huge amount of data, store them in databases, and perform the batch and real-time analytic. Moreover, there are various inside and outside attacks that threaten the security and privacy of smart cities, which make it essential to propose an effective security solution for smart cities. In this section, a combination of some keywords have leveraged to search the relevant studies

about smart cities: security and privacy/ smart city/ IoT/ big data/ cloud/ cloud of things/fog and edge. We classified the existing security methods into two groups, such as: IoT-based solutions, and cloud-based solutions, as follows.

A. Secure Authentication and Access Control for IoT-Based Objects

The smart devices, like smart phones and sensing nodes, are responsible to collect data in the smart cities, suffer from resource limitation, e.g., energy resources and processing power. As a result, protecting the security of data in such devices requires proposing a lightweight cryptographic algorithm that incurs minimum computation cost on them.

Lie *et al.* [67] propose a lightweight authentication and access control scheme for IoTs (AC-IOT) on the basis of Elliptic Curve Cryptography (ECC) [115] to manage the key establishment and Role-Based Access Control (RBAC) model [116] to define the access control policies. The aim of authentication method is to determine the legitimate users who can gain access to the IoTs by using an OpenID technology, which allows to register users and open a unique account for logging into many diverse sites by authenticating a single identity provider. The RBAC model also guarantees that the certain data and resource are only accessible by the authorized users. This method classifies the users on the basis of their roles in this access control model that helps to simplify the authorization management. Although the proposed model is secure against eavesdropping, man-in-the-middle, and Key Control attacks, it incurs high computation cost on IoT devices, and it is vulnerable against replay attack.

The work presented in [117], namely registry based authentication for IOTs (R-IOT), addressed the security issues of Lei *et al.*'s method [67] by adding a registration phase, which permits users and a gateway node to exchange a shared secret key for secure login and authentication success. Moreover, to reduce the imposed computation cost of the mutual authentication on things, the users are prohibited to directly communicate to the things. This method protects the IoTs against several attacks, such as resist replay, man-in-the-middle, offline-password guessing, and session key establishment attacks. In [118], an efficient authentication and access control scheme (ECC-IoT) is proposed for the perception layer of the IoTs to decline the communication and computation cost on the objects. The main idea behind this method is to use the ECC-based authentication and the attribute-based cryptographic (ABC) to provide a mutual authentication between user and nodes, and achieve a flexible fine-grained access control. The most important component in the proposed architecture is a base station (BS), which is responsible for collecting data and controlling the sensor nodes.

Identity-based Capability (ICAP) [119] is a common way to design a access control for IoT-based smart cities. Mahalle *et al.* [120] were the first to propose an authorization and access control approach, namely Identity driven Capability-based Access Control (ICAC), for IoT devices on the basis of ICAP. The main idea behind this method is to generate a capability for each device on the basis of the device identity, which is generated by using the media access control address for unique identification, and the contextual information associated with the device. When an access request is received by a device, the integrity of the requesters' capability needs to be checked by one way hash function and then the access is granted if the integrity of capacity is approved. To detect the valid capability from the tampering and forgery one, the capabilities are exchanged in conjunction with a SHA-1 message digests. However, the performance of this method has not been checked to prove its effectiveness for constrain devices. The authors extended this idea in [121] by proposing an Identity Establishment and Capability-based Access Control (IECAC) protocol by using ECC for IoTs with the aim of preserving the security of IoTs against man in middle, replay, and denial of service attacks. To achieve this goal, a shred secret key is established between two IoT devices using Elliptical Curve Cryptography-Diffie Hellman (ECCDH) algorithm and a one-way authentication is designed to authenticate Device A to Device B based on the share secret key and Message Authentication Code (MAC). Finally, to issue the permission to access an existing device or resource, a capability, including a unique device identifier and access rights, is constructed based on ICAP. However, this method imposes high computation and communication overhead on constrained devices.

Gusmeroli *et al.* [122] propose a Capability-Based Access Control (CapBAC) in IoT based on Policy Decision Points (PDPs) that are asked by services to issue access permission and authorization decisions. To access a specific data source, the user requires to attach the capability token to the access request, and then the PDP makes a decision about the user's authorization on the basis of the user's capability and the internal rules of the requested data source. In [123], the CapBAC is improved for constrained environments by proposing a Distributed Capability-Based Access Control (DCapBAC) method without requiring any additional entity in which the authorization logic is embedded into the constrained devices by adapting the communication technologies and representation format. The DCapBAC method is constructed on the basis of authorization tokens and a set of access conditions that needs to be verified at the end device after presenting token. To achieve this goal, the authors use Java Script Object Notation (JSON) [124] as a representation format for the capability token, which needs to be attached in access requests, and an optimized ECC [125] for authentication.

The method proposed in [126] presents an integral scenario that provides the security management (SM) of a constrained device during its life cycle. This method is constructed by using a lightweight version of Extensible Authentication Protocol Over LAN (EAPOL) [127] with aim of initiating a security bootstrapping process based on standard technologies (e.g., [128] and [129]) and obtaining authorization tokens [123] by extending with Extensible Access Control Markup Language (XACML)-based authorization procedures [130]. The lightweight authorization tokens are also used in this method (SM-EAPOL) to provide an end-to-end secure communication between constrained devices.

TABLE VI
COMPARISON OF THE AUTHENTICATION AND ACCESS CONTROL METHODS FOR IOT-BASED OBJECTS

Methods	Objectives	Drawbacks
AC-IOT [67]	A lightweight authentication and access control method for IoTs based on ECC and RBAC.	1) High computation overhead; 2) Cannot support data error
R-IOT [117]	Incurring less computation cost than other schemes by prohibiting users from directly connecting to the things, It also is secure against resist replay, man-in-the-middle, offline-password guessing, and session key establishment attacks.	Connection-oriented model encounters major limitations, Intermittent connectivity may render protocols unavailable during long periods of time
ECC-IoT [118]	An authentication and access control scheme for the perception layer of IoT by using ECC and ABC to provide efficient key establishment.	It is a theoretic method and it requires a complex management, which makes it impractical for resource constrained devices.
ICAC [120]	An authentication and access control scheme for the perception layer of IoT based on CAC and SHA-1 to preserve the security of capabilities against tampering or forgery attacks.	The performance of the method has not been check for constrained devices.
IECAC [121]	An authentication scheme to preserve the security of IoT devices against against man in middle, replay, and denial of service attacks.	Imposes high computation and communication overhead on constrained devices.
CapBAC [122]	Externalizing the authorization decisions in a central entity that help to issue privileges to be imposed on the end devices.	It requires a a central entity for communicating with IoT devices.
DCapBAC [123]	A distributed authorization approach for constrained devices by adapting the communication technologies such as CoAP and 6LoWPAN, optimized ECC, and data-interchange format, It also uses JSON as representation format for the token.	It cannot provide trust mechanisms, which considers the trustworthiness of the involved IoT devices for making access control decision.
SM-EAPOL [126]	An authentication approach based on based on EAP over LAN to establish keys for developed Datagram TLS.	The constrained devices require to implement and execute the EAPOL protocol in addition to DTLS, which makes it unsuitable for such devices

The comparison of the existing authentication and access Control methods for IoT-based objects is presented in Table VI.

B. Preventing Data Over-Collection in Smart Cities

Data over-collection is a crucial issue of the smart cities in which the mobile applications tend to collect data more than enough on their original functions (data leak) and transfer them to the untrsuted third parties. There are two different ways to cope with the data leak issue in mobile applications, such as detection and prevention methods, and user awareness methods.

Egele *et al.* [131] were the first to propose a static analysis method, namely PiOS, for detecting possible data privacy breaches in iOS applications. The main idea behind this method is to identify code paths that are used by application to access and transmit the sensitive information on the basis of analyzing the data flow and reconstructing the control flow graph of the application. In other words, it requires to carry out data flow analysis within the identified code paths to confirm whether sensitive information is flowing from the source functions that access the sensitive data to the sink functions that transmit the data to third parties. Gilbert *et al.* [132] design a security testing and validation system, namely AppInspector, based on a commodity cloud infrastructure for emulating the smartphone with the aim of dynamically track information flows and actions. The AppInspector relies on tracking two types of data flows: (i) Explicit flows: for tracking the propagation of sensitive information over the applications, external libraries, and system components through direct data dependencies, and (ii) Implicit flows: for tracking the propagation of private information that affects the control flow of the program or updates a public variable. In [133], a system-wide dynamic taint tracking and analysis platform, namely TaintDroid, is proposed to identify whether untrusted android applications endanger the privacy of users by manipulating the sensitive personal data or transferring them to third parties. To achieve this goal, the privacy-sensitive data from multiple sources are automatically labeled as sensitive data propagates through program variables, files, and interprocess messages. As a result, if the applications want to send such data over the network or any leaves the system, TaintDroid is able to detect by logging the data's labels. The TaintDroid method leverages the VM interpreter to deliver variable-level tracking within the application code to prevent the taint explosion observed in the x86 instruction set, message-level tracking between applications to extend the analysis system-wide, and file-level tracking to ensure persistent information conservatively retains its taint markings. The main drawback of the TaintDroid method is that protecting the sensitive data tends at the real-time may be impossible by the time a leak has been detected and analyzed.

Enck *et al.* [134] were the first to propose a user-aware security framework, namely Kirin, for enforcing the security policy, which transcends android applications, and safeguarding that policy compliant applications are only able to be installed by providing a self-certification process during the installation. The kirin has the capability to detect unconfident policy configuration in Android's framework by evaluating simple security requirement results in reducing the necessity to defer install-time decisions to the user. However, the implicit flows created by control structures have not been considered in this application for reducing the runtime cost. Moreover, it is impractical to identify potential information leaks by dynamically executing all execution paths of these applications. Xiao *et al.* [135] addressed these issues by proposing a user-ware privacy control approach to determine the usage of private information inside applications based on information

TABLE VII
COMPARISON OF DATA OVER-COLLECTION PREVENTION METHODS FOR IOT-BASED SMART CITIES

Methods	Objectives	Drawbacks
PiOS [131]	Uses static analysis to prove that the majority of ios applications do access the private information of users by creating control-flow graphs	The user reaction to prompts or cues about privacy is vague, the effectiveness of the proposed method that enables users to make informed choices is not proved.
AppInspector [132]	Uses End-user license agreements(EULA) to identify sensitive data leakage by showing notification during execution.	The majority of mobile application does not provide EULA during the data transmission.
TaintDroid [133]	As a dynamic taint analysis tool is used for tracking the privacy of sensitive information-flow within third-party android application at four levels of granularity: variable-level, method-level, message-level and file-level.	Dynamic analysis incurs large amount of computation cost on the smartphones, protecting the sensitive data tends at the real-time may be impossible by the time a leak has been detected and analyzed.
Kirin [134]	Detects application that needs dangerous combinations of permissions, provides a list of potential data flows across applications	Unable to identify local security enforcements made by applications, suffers from fails positive, cannot provide reliable decisions for automatic security enforcements.
[135]	A semi-automatic approach that uses user-driven access control mechanism to protect the user privacy by allowing users to select among real information, anonymized information, or abort execution.	The proposed static analysis is unable to handle implicit control flows.
[79]	Provides an access control privilege for the applications, which need to access the user's sensitive information in the cloud computing.	Incurs high computation and communication overhead on the users and CSP.

flow computation [136] and classification as safe and unsafe. When an application is running for the first time, this approach permits the user to use the application before giving access to real information, or prevents unintended access to a resource. This method also classifies the information as safe on the basis of a tamper analysis in which the untampered private information only reveals for the safe flows to preserve the privacy and minimize the decisions required from users. In other words, this approach is able to follow whether private data is concealed before escaping through output channels.

Although these methods may reduce the possibility of data leakage from mobile devices, storing sensitive data on mobile devices puts the data at risk. The best way to cope with this issue is to outsource the data to cloud computing to improve the data security of users. Li *et al.* [143] design a mobile-cloud framework in which the smartphone is only responsible for performing the basic operations of applications while the cloud service provider (CSP) deals with managing, encrypting, and decrypting the data, and providing fine-grained access control. The CSP provides an opportunity for smartphone users to store their data on the different level of storage solutions for sensitive or normal data. When an application wants to access a user's data, a request has to be sent to the CSP that provides fine grained permission authorizations for the applications. If the application be authorized by the CSP, the user's encrypted data are decrypted and transferred to the application. This method classifies the security level of data into five levels, such as extreme high, high, normal, low, and extreme low to authorizing the permissions to applications. Then, by calculating security risk of data and applications, it is possible to judge whether the security risk is outstripped and authorization fails. Fig. 4 shows the overall mobile-cloud framework for preventing the data over-collection.

The comparison of data over-collection prevention methods for IoT-based smart cities is presented in Table VII.

C. Secure Frameworks of IoT-Based Smart Cities

Chakrabarty and Engels [137] design a secure IoT-based architecture for smart cities to mitigate the vulnerabilities

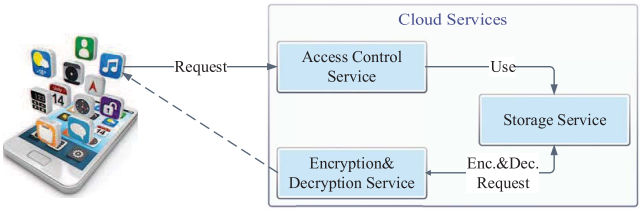

Fig. 4. The mobile-cloud framework for preventing data over-collection.

of tradition IoT networks at the Link and Network layers. This architecture consists of four main components: (i) Black Network: indicates a network for securing the metadata associated with each frame or packet in an IoT protocol in which the transmitted data through Link layer of IoT is encrypted by using Grain128a or Advanced Encryption Standard (AES) in the EAX or OFB modes. As a result, this component can preserve the privacy, confidentiality, integrity of data because of authenticating and securing the communications through the link layer and the network layer. (ii) Trusted SDN Controller: is responsible to manage anonymous data flow across IoT nodes and manage sleep and wake cycles of such nodes. (iii) Unified Registry: provides a database for the existing heterogeneous network devices (e.g., sensors, gateways and nodes) through the smart cities and their attributes that can be used for identity management, authentication, authorization and accounting. (iv) Key Management System: is known as an essential part of each security architecture for securely generating, managing, storing, communication, and distributing the symmetric cryptographic keys. This architecture leverages the hierarchical key management system to efficiently and securely supports key distribution among authorized devices. Fig. 5 shows the different components of the proposed IoT-based architecture for smart cities.

D. Security Frameworks of Cloud-Based Smart Cities

The integration of cloud computing and the Internet of Things provides a great opportunity for smart cities to overcome the existing issues for storing and analyzing the huge

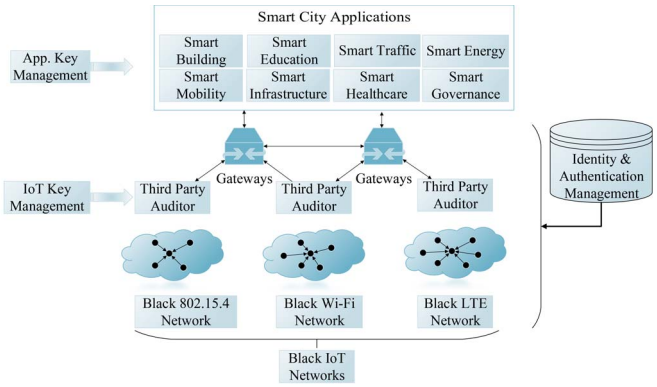

Fig. 5. Secure IoT architecture for smart cities.

amount of large-scale data in the smart cities. However, this integration provides some security issues and challenges, as a main obstacle that forces us to deal with.

Providing a secure communication between the components of cloud-based smart cities is a significant issue. Bhattasali *et al.* [84] design a secure data sharing for cloud-based smart cities to deal with the data security communication issue between two parties by using Lightweight Identity Based Cryptography (LIBC) [138] to perform encryption and decryption in real time. The LIBC consists of four distinct phases: (i) Setup phase: to generate the require keys and auxiliary parameters, (ii) Extraction phase: in which the public key, private key, and public parameters are generated for each user based on the user identity and transmitted to the users, (iii) Encryption phase: during this phase, user A is able to encrypt a message for user B on the basis of Tate pairing computation, signs it by choosing a random number, and transfers it to the CSP, and (iv) Decryption phase: in this phase, the encrypted message is downloaded by user B and decrypts the message by her own private key. In [63], a secure communication scheme for secure data exchange among different components is presented for cloud-based smart cities in which the IoT devices are categorized based on their communication types into two groups: one-way communication devices that require basic operations, and two ways communication devices, which are used for monitoring and controlling purpose. The applications in each group are interconnected with a group leader using technologies like ZigBee or Wi-Fi that are directly connected with the CSP using a public network such as the Internet. As a result, the CSP can manage all devices and send a unique command to each of them. The author leverages a symmetric key cryptography to provide a secure communication between the applications in each group and between the group leaders and the CSP. For example, when the CSP needs to transfer a message to a device in the group 1, the CSP encrypts the message (m) along with a time stamp (t_1) using the symmetrical key shared (GK_1) between the CSP and the device in Group 1 , and then concatenates the result with the ID of the group 1 ($D_1 = ID_{G_1}.Enc_{GK_1}(m, t_1)$). Since the message must be transmitted to the appliance via the group leader (GL_1) of the first group 1, the CSP re-encrypts D_1 along with a time stamp (t_2) using a shared key with the GL_1, GLK_1, concatenates it with the ID of GL_1 ($D_2 = ID_{GL_1}.Enc_{GLK_1}(D_1, t_2)$), and finally sends ($D_1, D_2$) to the GL_1.

Designing a secure framework for smart cities is a challenging area. Khan *et al.* [139] propose a framework for preserving the security and privacy of data during data acquisition, transmission, processing and legitimate service provisioning in smart cities on the basis of the stakeholder model, which they identified by using onion model approach. This framework consists of three layers, such as smart city inhabitant, governmental control domain layer, and service provider layers. (i) Smart city inhabitants layer: is responsible to provide the security and privacy of inhabitants, collected data from different resources, and provisioned services. This layer contains different components, such as the authenticator for validating the authentication of inhabitants or service providers, services and application component to provide tamper with resistant service provisioning, policy decision point component to ensure that data privacy is considered before accessing or sharing data, authorization and data confidentiality components to provide data access control and ensure sensitive data are not access by malicious services or third party, and the data anonymization components to ensure the separation of inhabitants from the sensed data. (ii) Governmental Control Domain (GCD) layer: Operates as a regulatory authority deals with ensuring the services providers and citizens are working according to predefined regulations and policies. The GCD layer includes several components, such as provider verification, seamless sensed data analysis, linked open data, and service integrity checker. The service provider verification is responsible to provide legitimate and trustable service provisioning. The seamless sensed data analysis guarantees that the included entities follow their limitations by implementing a proper audit trail mechanism. The linked open data as the next component of the GCD stores the information, which are managed by the regulatory authority to be only accessible by the authorized service providers. The service integrity checker components is in charge of issuing credentials for devices, services and citizens of smart cities for ensuring that the service providers can trust the data sources. These credentials also help to filter the sources that gerents fake data to prevent forge service experience. (iii) Service provider layer: is in charge of providing service provisioning and secure and privacy-aware data sharing in untrusted area. This layer involves the following components: service and application provisioning component that provides an execution environment for services, data repositories component to help the service provider to securely access data repositories and securely share data with other service providers. The service provider layer has to use divers measurements, such as secure data sharing and processing, fine-grained controlled over shared data with secure data revocation, and secure key management.

Henze *et al.* [94] present a User-driven Privacy Enforcement for Cloud-based Services (UPECSI) to preserve the privacy of sensitive data of users through the cloud-based smart cities by integrating the privacy functionality into the development process of cloud services. The UPECSI approach includes the following components: (i) Model driven privacy as a technique

TABLE VIII
COMPARISON OF CLOUD-BASED AND IOT-BASED FRAMEWORKS FOR SMART CITIES

Type	Methods	Conf.	Integ.	Authen.	Autho.	Trans.	Anonym.	Assumptions & Drawbacks
Cloud-based	[84]	✓	✓					Only securing communication using LIBC
	[63]	✓	✓					Only securing communication using symmetric cryptography
	[139]	✓	✓	✓	✓		✓	Not applicable for securing online analytic
	UPECSI [94]	✓	✓	✓	✓	✓		Not applicable for securing online analytic
IoT- based	[137]	✓	✓	✓	✓			Not applicable for securing batch and online analytic

to integrate the privacy functionality into the development of cloud service, (ii) Interpretation component that helps users to configure their individual privacy setting, and (iii) Privacy Enforcement Points (PEP) component, which are located in the IoT network gateways and deals with enforcing users' privacy requirements before uploading the sensitive data to the CSP. The main idea behind this method is that the model driven privacy firstly extracts a privacy policy, which involves the require service information and general liability disclaimers for each service. Then, the service developer provides information during the development process to be used by the third party to audit the cloud service and monitor data usage. When a service is detected to be eligible to access the collected data from different resources in smart cities, the user will be able to make an overview on the audited policy as well as a default privacy configuration suggested by the third party on her devices (e.g., laptop and smartphone). The user is also able to decide whether to delegate the data access privilege to a service. Considering the user decision, finally the user can control the access to the sensitive data by using the PEP. To protect the data and access control, the PEP encrypts the data by using a symmetric data protection key before outsourcing to the cloud.

Table VIII shows the comparison of cloud-based and IoT-based frameworks for smart cities on the basis of different attributes, such as confidentiality, integrity, authentication, authorization & access control, transparency, and anonymization.

VII. OPEN ISSUES AND CHALLENGES

Smart city has been emerged as a new paradigm recently and there are a few researchers in different aspect of this area. Although security and privacy are known as the most important parts of smart cities, they have not been sufficiently considered by researchers. This section provides some open issues that can be used as a future direction.

A. Lightweight Methods for Big Data Processing

Although big data is an inseparable part of the smart cities, integrating these two concepts needs to tackle several challenges. This is because the deployed sensors throughout cities collect a huge volume of data in distinct formats from different sectors of cities such as traffic, homes, education, manufactures, and health-care centers. The collected data usually is stored in NoSQL databases regularly, are used to perform real time or batch processing to detect the events. Batch data processing indicates an effective way to process and analyze a huge volume of data that is collected over a period of time and stored in NoSQL databases. In contrast, real-time data processing includes a continuous input, analyze, and output of data flows with high performance in which the processing of data has to be in a small period of time or near real time. Recently, some of the researchers have proposed big data analytic frameworks for smart cities (e.g., [140]–[143]) to overcome the big data issues; however, the majority of such frameworks are unable to support security and privacy of data through the different layers of their architectures. Preserving the security and privacy of such an amount of data requires a highly efficient and lightweight cryptographic algorithm, which incurs minimum computation cost on resource constrained devices.

B. Secure Data Outsourcing

Cloud-based frameworks provide an efficient way to tackle the storage overhead issue in the smart cities. Despite the fact that the cost of storage hardware is decreasing, the management of such huge storage is more complex and constitutes approximately 75% of the total ownership cost [144], [145]. In other words, the huge volume of data collected by IoT devices in the smart cities can be outsourced to the cloud storages and delegate the management of data to the CSP. However, the cloud is inherently neither secure nor reliable, and it raises new challenges to the integrity of outsourced data in cloud computing. To address this issue, Remote Data Auditing (RDA) methods have been proposed in which the data owner is able to check the integrity of outsourced data without having to download the whole data. Although there are different types of RDA methods (e.g., [146]–[148]) to check the integrity of outsourced data, the majority of such methods are inapplicable for supporting big data through smart cities.

C. Secure and Intelligent Participatory Sensing for Smart Cities

Participatory sensing is the process whereby individuals and communities use evermore-capable mobile phones and cloud services to collect and analyze systematic data for use in discovery [149]. The participatory sensing has also the capability to provide the adjacent sign and information regarding environmental parameters gathered by the end-users that form a social currency [50]. As a result, the smart city applications, such as health-care and energy controlling, are able to directly

compare the available data with the collected online data over a fixed infrastructure sensor network. In addition, such applications can use an experience feedback of end-users about a given environmental parameter. However, the existing infrastructure of smart cities prevents to use these features, and it requires to design a new framework for smart cities to be able to use the great potential of participatory sensing to collect data from the reliable resources and perform real-time analysis.

D. Security Risk Management and Mitigation

The smart cities rely on the sensing devices that usually deployed in the harsh environments surrounding by a numerous number of security threats. Therefore, it is essential to design a method to mitigate such threats for facilitating the smart cities applications and making more citizens interest in using the smart city applications. However, due to the heterogeneity of sensing devices and networks in the smart cities, designing a comprehensive risk mitigation scheme is a critical challenging. Although there are some risk mitigation models (e.g., [150]–[152]) for different networks and sensing devices, it is commonly impossible to use a combination of such schemes for smart cities.

Designing a security mitigation method for the cloud-base smart city is essential, because the majority of applications migrate from the information to the virtual servers without considering the level of security level of data. In other words, the smart cities need a security mitigation model to decide whether migrating from the data to the virtual server considering with the degree of sensitivity of data.

E. The Application of Fog Computing in Smart Cities

The IoT devices usually collect huge amount of data, which make it very challenging for smart cities to locally store and manage such large-scale data. Although cloud computing provided a way to address this issue, transferring the large-scale data to the cloud is costly in terms of communication, bandwidth, latency and storage. To overcome this issue, IBM suggested fog computing as a new concept in which instead of sending such amount of data to the cloud, it is possible to process the data at the edge of the network and in the vicinity of users [153].

Fog computing has a great application to build a sustainable smart city. There are some case studies which can prove this opinion: (i) Smart agriculture in Phenonet Australia [154] where in fog computing plays a vital role in acquiring data efficiently about plant growing, performance information and weather conditions; (ii) Smart Healthcare: a wearable light-weight sensor kit has been designed to collect Electroencephalography data of some volunteers during their exercise and performed pre-processing on their smartphones as fog nodes to reduce latency [155]; and (iii) Smart Water Management: the collected data from deployed sensors and GPS devices can be analyzed by using fog gateways [156].

Despite Fog computing can provide significant benefits for smart cities, it makes the smart cities vulnerable to several security issues and challenges in virtualization, Web security, and data security [157]. This is because fog nodes are suffering from limitation of computing resources, which makes it difficult for proposing security solutions [158]. The fog nodes are usually more accessible than cloud data centers results in increasing the probability of cyber-attacks. Fog nodes also are more attractive for attackers because of collecting huge volume of sensitive data from different resources [159].

F. Adoption With Government Policies

IoT devices in smart cities are responsible to collect the information and transfer them to local or remote data centers for performing batch or online data analysis. The city government usually is able to manage the majority of this transformation by using the policies. However, collecting more data including personal information of citizens, faces the smart cities with the privacy issues. As a result, law enforcement agencies are more interested in gaining access to such information without considering proper security [160]. The smart cities may also sell the collected information to third party companies without taking permission from residents. Some of the cities, such as New York, London and Dubai, recently set up new video surveillance to capture crime and terrorist attacks. Since these systems violate the privacy of citizens and civil rights by recording the citizen movements and enabling arbitrary search, they put the smart cities at risk. Therefore, implementing new smart city technologies require new government policies for increasing transparency to make a balance between benefits and security risks [161].

VIII. Conclusion

In this paper, we have characterized, and categorized wide-range areas of research related to the smart city, with the aim of focusing on security and privacy issues and the ways to address them. We began by explaining the history of smart city concept based on digital cities and ICT cities and comparing their features. Then, we have taxonomized the smart city on the basis of architecture, key components, pillars, and applications. Moreover, we have presented a comprehensive survey on security and privacy of smart cities with focusing on security requirements, issue and challenges. We have also critically reviewed and examined the potential solutions for addressing the security and privacy issues of the smart cities with the aim of discovering some of the advantages and disadvantages, highlighting their similarities and differences, and recognizing the research gap in the architecture. Finally, numerous open issues have been identified as the prominent challenges for future research directions.

Acknowledgment

The authors thank the reviewers for their detailed reviews and constructive comments, which have helped to greatly improve the quality of this paper.

REFERENCES

[1] "World urbanization prospects: The 2014 revision, highlights (ST/ESA/SER.A/352)," Dept. Econ. Soc. Affairs Popul. Div., United Nat., New York, NY, USA, Rep. 352, 2014. [Online]. Available: https://esa.un.org/unpd/wup/Publications/Files/WUP2014-Highlights.pdf

[2] P. Neirotti, A. De Marco, A. C. Cagliano, G. Mangano, and F. Scorrano, "Current trends in smart city initiatives: Some stylised facts," *Cities*, vol. 38, pp. 25–36, Jun. 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0264275113001935

[3] J. M. Barrionuevo, P. Berrone, and J. E. Ricart, "Smart cities, sustainable progress," *IESE Insight*, vol. 14, no. 14, pp. 50–57, 2012.

[4] C. Benevolo, R. P. Dameri, and B. D'Auria, *Smart Mobility in Smart City*. Cham, Switzerland: Springer Int., 2016, pp. 13–28, doi: 10.1007/978-3-319-23784-8_2.

[5] H. Chourabi *et al.*, "Understanding smart cities: An integrative framework," in *Proc. 45th Hawaii Int. Conf. Syst. Sci.*, Jan. 2012, pp. 2289–2297.

[6] M. Perevezentsev, "Strategic opportunity analysis of the global smart city market," Frost Sullivan, San Antonio, TX, USA, Rep., 2013.

[7] V. Albino, U. Berardi, and R. M. Dangelico, "Smart cities: Definitions, dimensions, performance, and initiatives," *J. Urban Technol.*, vol. 22, no. 1, pp. 3–21, 2015, doi: 10.1080/10630732.2014.942092.

[8] L. G. Anthopoulos, "Understanding the smart city domain: A literature review," in *Transforming City Governments for Successful Smart Cities*, M. P. Rodríguez-Bolívar, Ed. Cham, Switzerland: Springer Int., 2015, pp. 9–21, doi: 10.1007/978-3-319-03167-5_2.

[9] "Smart cities require smarter cybersecurity," ForeScout Technol., San Jose, CA, USA, Rep., 2016. [Online]. Available: http://www.govtech.com/library/papers/Smart-Cities-Require-Smarter-Cybersecurity-80678.html

[10] K. Zhang *et al.*, "Security and privacy in smart city applications: Challenges and solutions," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 122–129, Jan. 2017.

[11] Y. He, F. R. Yu, N. Zhao, V. C. M. Leung, and H. Yin, "Software-defined networks with mobile edge computing and caching for smart cities: A big data deep reinforcement learning approach," *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 31–37, Dec. 2017.

[12] A. Bartoli *et al.*, "Security and privacy in your smart city," in *Proc. Barcelona Smart Cities Congr.*, 2011, pp. 1–6.

[13] R. Kitchin, "Getting smarter about smart cities: Improving data privacy and data security," Dept. Taoiseach Behalf Govt. Data Forum, Maynooth Univ., Maynooth, Ireland, Rep., 2016. [Online]. Available: http://eprints.maynoothuniversity.ie/7242/1/Smart

[14] C. D. E. Lévy-Bencheton, "Cyber security for smart cities—An architecture model for public transport," Eur. Union Agency Netw. Inf. Security, Heraklion, Greece, Rep., 2016. [Online]. Available: https://www.enisa.europa.eu/publications/smart-cities-architecture-model/at_download/fullReport

[15] A. Solanas *et al.*, "Smart health: A context-aware health paradigm within smart cities," *IEEE Commun. Mag.*, vol. 52, no. 8, pp. 74–81, Aug. 2014.

[16] X. Li *et al.*, "Smart community: An Internet of Things application," *IEEE Commun. Mag.*, vol. 49, no. 11, pp. 68–75, Nov. 2011.

[17] R. Kitchin, "The real-time city? Big data and smart urbanism," *GeoJournal*, vol. 79, no. 1, pp. 1–14, 2014, doi: 10.1007/s10708-013-9516-8.

[18] A. M. Townsend, *Smart Cities: Big Data, Civic Hackers, and the Quest for A New Utopia*. New York, NY, USA: W. W. Norton & Company, 2013.

[19] H. Schaffers *et al.*, "Smart cities and the future Internet: Towards cooperation frameworks for open innovation," in *The Future Internet: Future Internet Assembly 2011: Achievements and Technological Promises*. Heidelberg, Germany: Springer, 2011, pp. 431–446, doi: 10.1007/978-3-642-20898-0_31.

[20] M. Batty *et al.*, "Smart cities of the future," *Eur. Phys. J. Spec. Topics*, vol. 214, no. 1, pp. 481–518, 2012.

[21] A. Caragliu, C. Del Bo, and P. Nijkamp, "Smart cities in Europe, series research memoranda," in *Proc. 3rd Cent. Eur. Conf. Regional Sci. (CERS)*, 2009, pp. 45–58.

[22] J. An *et al.*, "Achieving sustainable ultra-dense heterogeneous networks for 5G," *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 84–90, Dec. 2017.

[23] J. Wu, S. Guo, H. Huang, W. Liu, and Y. Xiang, "Information and communications technologies for sustainable development goals: State-of-the-art, needs and perspectives," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2389–2406, 3rd Quart., 2018.

[24] T. Bakıcı, E. Almirall, and J. Wareham, "A smart city initiative: The case of Barcelona," *J. Knowl. Econ.*, vol. 4, no. 2, pp. 135–148, 2013, doi: 10.1007/s13132-012-0084-9.

[25] T. M. Chen, "Smart grids, smart cities need better networks [Editor's Note]," *IEEE Netw.*, vol. 24, no. 2, pp. 2–3, Mar./Apr. 2010.

[26] C. Harrison *et al.*, "Foundations for smarter cities," *IBM J. Res. Develop.*, vol. 54, no. 4, pp. 1–16, Jul./Aug. 2010.

[27] G. C. Lazaroiu and M. Roscia, "Definition methodology for the smart cities model," *Energy*, vol. 47, no. 1, pp. 326–332, 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0360544212007062

[28] A. Caragliu, C. Del Bo, and P. Nijkamp, "Smart cities in Europe," *J. Urban Technol.*, vol. 18, no. 2, pp. 65–82, 2011, doi: 10.1080/10630732.2011.601117.

[29] J. M. Eger, "Smart growth, smart cities, and the crisis at the pump a worldwide phenomenon," *I-WAYS Dig. Electron. Commerce Policy Regul.*, vol. 32, no. 1, pp. 47–53, 2009.

[30] A. Velosa, B. Tratz-Ryan, L. Anavitarte, and H. Fernando, "Market trends: Smart cities are the new revenue Frontier for technology providers," Gartner, Stamford, CT, USA, Rep., 2011. [Online]. Available: https://www.gartner.com/doc/1615214/market-trends-smart-cities-new

[31] R. Giffinger, C. Fertner, H. Kramar, and E. Meijers, "City-ranking of European medium-sized cities," Centre Regional Sci., Technische Universität Wien, Vienna, Austria, Rep., 2007.

[32] K. Kourtit and P. Nijkamp, "Smart cities in the innovation age," *Innov. Eur. J. Soc. Sci. Res.*, vol. 25, no. 2, pp. 93–95, 2012, doi: 10.1080/13511610.2012.660331.

[33] P. Lombardi, S. Giordano, H. Farouh, and W. Yousef, "Modelling the smart city performance," *Innov. Eur. J. Soc. Sci. Res.*, vol. 25, no. 2, pp. 137–149, 2012, doi: 10.1080/13511610.2012.660325.

[34] L.-G. Cretu, "Smart cities design using event-driven paradigm and semantic Web," *Informatica Economica*, vol. 16, no. 4, pp. 57–67, 2012.

[35] S. Zygiaris, "Smart city reference model: Assisting planners to conceptualize the building of smart city innovation ecosystems," *J. Knowl. Econ.*, vol. 4, no. 2, pp. 217–231, 2013, doi: 10.1007/s13132-012-0089-4.

[36] M.-L. Marsal-Llacuna, J. Colomer-Llinàs, and J. Meléndez-Frigola, "Lessons in urban monitoring taken from sustainable and livable cities to better address the smart cities initiative," *Technol. Forecast. Soc. Change*, vol. 90, pp. 611–622, Jan. 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0040162514000456

[37] "Smart cities and infrastructure," UNCTAD, Geneva, Switzerland, Rep., 2016. [Online]. Available: http://unctad.org/meetings/en/SessionalDocuments/ecn162016d2_en.pdf

[38] B. Cooper and D. Rawat, "Cyber security—A necessary pillar of smart cities," Ernst & Young, London, U.K., Rep., 2016. [Online]. Available: http://www.ey.com/Publication/vwLUAssets/ey-cyber-security-a-necessary-pillar-of-smart-cities/$FILE/ey-cyber-security-a-necessary-pillar-of-smart-cities.pdf

[39] H. C. Christiansen and E. Kongsmark, "Becoming a smart energy city, state of the art and ambition," Eur. Union, Rep., 2015. [Online]. Available: http://urbantransform.eu/wp-content/uploads/sites/2/2015/07/WP1-revised-final-report.march-2015.pdf

[40] "Smart buildings enable smart cities," Wipro, Bengaluru, India, Rep., 2016. [Online]. Available: http://www.wipro.com/documents/insights/Smart-Buildings-Enable-Smart-Cities.pdf

[41] T. Okuda, S. Hirasawa, N. Matsukuma, T. Fukumoto, and A. Shimura, "Smart mobility for smart cities," *Hitachi Rev.*, vol. 61, no. 3, pp. 141–146, 2012.

[42] "Smart cities: Regional perspectives," Rep., 2015.

[43] (2017). *Defining the Cities of Tomorrow: Predictions for 2017*. [Online]. Available: http://www.ibigroup.com/new-smart-cities-landing-page/education-smart-cities/

[44] D. Peeples. (2016). *Smart Education: Why Microsoft is Taking a Video Game to the Classroom*. [Online]. Available: http://smartcitiescouncil.com/article/smart-education-why-microsoft-taking-video-game-classroom

[45] D. Hill, "On the smart city: Or, a 'manifesto' for smart citizens instead," City Sound, London, U.K., Rep., 2013. [Online]. Available: http://www.cityofsound.com/blog/2013/02/on-the-smart-city-a-call-for-smart-citizens-instead.html

[46] "Smart cities guide: Traffic management," GSMA, London, U.K., Rep., 2016. [Online]. Available: https://www.gsma.com/iot/gsma-smart-cities-guide-traffic-management/

[47] R. Soderbery, "How many things are currently connected to the 'Internet of Things' (IoT)?" Forbes, New York, NY, USA, Rep., 2013. [Online]. Available: https://www.forbes.com/sites/quora/2013/01/07/how-many-things-are-currently-connected-to-the-internet-of-things-iot/#452889bcbd2d

[48] A. Nordrum, "Popular Internet of Things forecast of 50 billion devices by 2020 is outdated," IEEE Spectr., New York, NY, USA, Rep., 2016. [Online]. Available: http://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated

[49] K. Hamedani, L. Liu, R. Atat, J. Wu, and Y. Yi, "Reservoir computing meets smart grids: Attack detection using delayed feedback networks," *IEEE Trans. Ind. Informat.*, vol. 14, no. 2, pp. 734–743, Feb. 2018.

[50] Q. Shi, W. Xu, J. Wu, E. Song, and Y. Wang, "Secure beamforming for MIMO broadcasting with wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2841–2853, May 2015.

[51] N. Liu, J. Chen, L. Zhu, J. Zhang, and Y. He, "A key management scheme for secure communications of advanced metering infrastructure in smart grid," *IEEE Trans. Ind. Electron.*, vol. 60, no. 10, pp. 4746–4756, Oct. 2013.

[52] Z. Wan, G. Wang, Y. Yang, and S. Shi, "SKM: Scalable key management for advanced metering infrastructure in smart grids," *IEEE Trans. Ind. Electron.*, vol. 61, no. 12, pp. 7055–7066, Dec. 2014.

[53] "Cyber security in the era of the smart home," Rambus Inc., Sunnyvale, CA, USA, Rep., 2016. [Online]. Available: http://info.rambus.com/hubfs/rambus.com/Gated-Content/Cryptography/Cyber-Security-in-the-Era-of-the-Smart-Home-White-Paper.pdf?hsCtaTracking=bf8d7eb4-8b77-4a07-8ae2-759100c676a6%7C69c7a89b-6dfb-4926-8c38-860b7fd1eff5

[54] "What is UEFI secure boot?" Fedora, New York, NY, USA, Rep., Apr. 2017. [Online]. Available: https://docs.fedoraproject.org/en-US/Fedora/18/html/UEFI_Secure_Boot_Guide/chap-UEFI_Secure_Boot_Guide-What_is_Secure_Boot.html

[55] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jul. 2015, pp. 180–187.

[56] K. Yuksel, "Universal hash functions for emerging ultra-low-power networks," Ph.D. dissertation, Elect. Comput. Eng., Worcester Polytechnic Inst., Worcester, MA, USA, 2004. [Online]. Available: https://web.wpi.edu/Pubs/ETD/Available/etd-0428104-195331/unrestricted/yuksel.pdf

[57] J.-P. Kaps, K. Yuksel, and B. Sunar, "Energy scalable universal hashing," *IEEE Trans. Comput.*, vol. 54, no. 12, pp. 1484–1495, Dec. 2005.

[58] T. Berardi *et al.*, "Customer cloud architecture for big data and analytics," Cloud Stand. Customer Council, Columbus, OH, USA, Rep., 2015. [Online]. Available: http://www.cloud-council.org/deliverables/CSCC-Cloud-Customer-Architecture-for-IoT.pdf

[59] *Cisco Security Monitoring, Analysis and Response System*. [Online]. Available: https://www.cisco.com/c/en/us/products/security/security-monitoring-analysis-response-system/index.html

[60] "Managing the IoT lifecycle from design through end-of-life," Wind Intel Company, Santa Clara, CA, USA, Rep., 2015. [Online]. Available: http://events.windriver.com/wrcd01/wrcm/2016/08/WP-managing-the-iot-lifecycle-from-design-through-end-of-life.pdf

[61] A. Sinaeepourfard, J. Garcia, X. Masip-Bruin, and E. Marin-Tordera, "A novel architecture for efficient fog to cloud data management in smart cities," in *Proc. IEEE 37th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jun. 2017, pp. 2622–2623.

[62] A. Amies, H. Sluiman, Q. G. Tong, and G. N. Liu, *Developing and Hosting Applications on the Cloud*. Upper Saddle River, NJ, USA: IBM Press book, 2012.

[63] A. Bashar, "Security in cloud of things (CoT)," in *Managing Big Data in Cloud Computing Environments*, M. Zongmin, Ed. Hershey, PA, USA: IGI Glob., 2016, pp. 46–70. [Online]. Available: http://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-4666-9834-5.ch003

[64] X. Zou, *IoT Devices are Hard to Patch: Here's Why and How to Deal With Security*, Techbeacon. [Online]. Available: https://techbeacon.com/iot-devices-are-hard-patch-heres-why-how-deal-security

[65] J.-M. Bohli, P. Langendörfer, and A. F. Skarmeta, "Security and privacy challenge in data aggregation for the IoT in smart cities," in *Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems*, O. Vermesan and P. Friess, Eds. Aalborg, Denmark: River, 2013, pp. 225–244.

[66] H. Wen *et al.*, "A cross-layer secure communication model based on discrete fractional Fourier transform (DFRFT)," *IEEE Trans. Emerg. Topics Comput.*, vol. 3, no. 1, pp. 119–126, Mar. 2015.

[67] J. Liu, Y. Xiao, and C. L. P. Chen, "Authentication and access control in the Internet of Things," in *Proc. 32nd Int. Conf. Distrib. Comput. Syst. Workshops*, 2012, pp. 588–592.

[68] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology*, G. R. Blakley and D. Chaum, Eds., vol. 196. Heidelberg, Germany: Springer, 1985, ch. 5, pp. 47–53, doi: 10.1007/3-540-39568-7_5.

[69] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. 13th ACM Conf. Comput. Commun. Security*. Alexandria, VA, USA, 2006, pp. 89–98.

[70] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-based access control models," *IEEE Comput.*, vol. 29, no. 2, pp. 38–47, Feb. 1996.

[71] M. Sookhak, F. R. Yu, M. K. Khan, Y. Xiang, and R. Buyya, "Attribute-based data access control in mobile cloud computing: Taxonomy and open issues," *Future Gener. Comput. Syst.*, vol. 72, pp. 273–287, Jul. 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X16302795

[72] J. Zang, K. Dummit, J. Graves, P. Lisker, and L. Sweeney, "Who knows what about me? A survey of behind the scenes personal data sharing to third parties by mobile apps," Technol. Sci., Rep., Oct. 2015. [Online]. Available: https://techscience.org/a/2015103001/

[73] Kanishk. (2017). *What is A Botnet Attack and How to Identify It? HaltDos Blogs*. [Online]. Available: https://blogs.haltdos.com/2017/03/28/botnet-attack-identify/

[74] J. Choi, C. Choi, B. Ko, and P. Kim, "A method of DDoS attack detection using HTTP packet pattern and rule engine in cloud computing environment," *Soft Comput.*, vol. 18, no. 9, pp. 1697–1703, Sep. 2014. [Online]. Available: https://doi.org/10.1007/s00500-014-1250-8

[75] Q. Liao, H. Li, S. Kang, and C. Liu, "Application layer DDoS attack detection using cluster with label based on sparse vector decomposition and rhythm matching," *Security Commun. Netw.*, vol. 8, no. 17, pp. 3111–3120, 2015, doi: 10.1002/sec.1236.

[76] W. Zhou, W. Jia, S. Wen, Y. Xiang, and W. Zhou, "Detection and defense of application-layer DDoS attacks in backbone Web traffic," *Future Gener. Comput. Syst.*, vol. 38, pp. 36–46, Sep. 2014.

[77] N. Z. Bawany and J. A. Shamsi, "Application layer DDoS attack defense framework for smart city using SDN," in *Proc. 3rd Int. Conf. Comput. Sci. Comput. Eng. Soc. Media (CSCESM)*, 2016, pp. 1–9.

[78] A. Barth, C. Jackson, and J. C. Mitchell, "Robust defenses for cross-site request forgery," in *Proc. 15th ACM Conf. Comput. Commun. Security*, Alexandria, VA, USA, 2008, pp. 75–88.

[79] Y. Li, W. Dai, Z. Ming, and M. Qiu, "Privacy protection for preventing data over-collection in smart city," *IEEE Trans. Comput.*, vol. 65, no. 5, pp. 1339–1350, May 2016.

[80] B. B. Gupta, S. Gupta, S. Gangwar, M. Kumar, and P. K. Meena, "Cross-site scripting (XSS) abuse and defense: Exploitation on several testing bed environments and its defense," *J. Inf. Privacy Security*, vol. 11, no. 2, pp. 118–136, 2015.

[81] J. Seibert, H. Okhravi, and E. Söderström, "Information leaks without memory disclosures: Remote side channel attacks on diversified code," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, Scottsdale, AZ, USA, 2014, pp. 54–65.

[82] L. R. Knudsen and M. J. B. Robshaw, "Brute force attacks," in *The Block Cipher Companion*. Heidelberg, Germany: Springer, 2011, pp. 95–108, doi: 10.1007/978-3-642-17342-4_5.

[83] M. Sookhak, A. Gani, M. K. Khan, and R. Buyya, "Dynamic remote data auditing for securing big data storage in cloud computing," *Inf. Sci.*, vol. 380, pp. 101–116, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0020025515006581

[84] T. Bhattasali, R. Chaki, and N. Chaki, "Secure and trusted Cloud of Things," in *Proc. Annu. IEEE India Conf. (INDICON)*, 2013, pp. 1–6.

[85] A. Rehman, S. Alqahtani, A. Altameem, and T. Saba, "Virtual machine security challenges: Case studies," *Int. J. Mach. Learn. Cybern.*, vol. 5, no. 5, pp. 729–742, 2014, doi: 10.1007/s13042-013-0166-4.

[86] Z. Gál *et al.*, "Internet of Things: Application areas and research results of the FIRST project," *Infocommun. J.*, vol. 6, no. 3, pp. 37–44, 2014.

[87] S. W. Oh and H. S. Kim, "Decentralized access permission control using resource-oriented architecture for the Web of Things," in *Proc. 16th Int. Conf. Adv. Commun. Technol.*, 2014, pp. 749–753.

[88] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context aware computing for the Internet of Things: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 414–454, 1st Quart., 2014.

[89] H. I. Kobo, A. M. Abu-Mahfouz, and G. P. Hancke, "A survey on software-defined wireless sensor networks: Challenges and design requirements," *IEEE Access*, vol. 5, pp. 1872–1899, 2017.

[90] H. Chaouchi, *The Internet of Things: Connecting Objects*. New York, NY, USA: Wiley, 2013.

[91] C. Stergiou, K. E. Psannis, B.-G. Kim, and B. Gupta, "Secure integration of IoT and cloud computing," *Future Gener. Comput. Syst.*, vol. 78, pp. 964–975, Jan. 2018.

[92] J. Parms, "More info, more problems: Privacy and security issues in the age of big data," Rep., 2017. [Online]. Available: https://www.business.com/articles/privacy-and-security-issues-in-the-age-of-big-data/

[93] D. Damopoulos, G. Kambourakis, M. Anagnostopoulos, S. Gritzalis, and J. H. Park, "User privacy and modern mobile services: Are they on the same path?" *Pers. Ubiquitous Comput.*, vol. 17, no. 7, pp. 1437–1448, 2013, doi: 10.1007/s00779-012-0579-1.

[94] M. Henze *et al.*, "A comprehensive approach to privacy in the cloud-based Internet of Things," *Future Gener. Comput. Syst.*, vol. 56, pp. 701–718, Mar. 2016.

[95] L. Hou *et al.*, "Internet of Things cloud: Architecture and implementation," *IEEE Commun. Mag.*, vol. 54, no. 12, pp. 32–39, Dec. 2016.

[96] L. Sun, J. Singh, and O. K. Hussain, "Service level agreement (SLA) assurance for cloud services: A survey from a transactional risk perspective," in *Proc. 10th Int. Conf. Adv. Mobile Comput. Multimedia*, 2012, pp. 263–266.

[97] A. Botta, W. de Donato, V. Persico, and A. Pescapé, "Integration of cloud computing and Internet of Things: A survey," *Future Gener. Comput. Syst.*, vol. 56, pp. 684–700, Mar. 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X15003015

[98] "Securing multi-tenancy and cloud computing," Juniper Netw., Sunnyvale, CA, USA, Rep., 2012. [Online]. Available: https://www.juniper.net/us/en/local/pdf/whitepapers/2000381-en.pdf

[99] H. Kumarage, I. Khalil, A. Alabdulatif, Z. Tari, and X. Yi, "Secure data analytics for cloud-integrated Internet of Things applications," *IEEE Cloud Comput.*, vol. 3, no. 2, pp. 46–56, Mar./Apr. 2016.

[100] "Guidance on the use of cloud computing," Inf. Commissioner's Office, Wilmslow, U.K., Rep., 2012. [Online]. Available: https://www.whitepapers.em360tech.com/white_paper/guidance-use-cloud-computing/

[101] R. A. Alshawish, S. A. M. Alfagih, and M. S. Musbah, "Big data applications in smart cities," in *Proc. Int. Conf. Eng. MIS (ICEMIS)*, Sep. 2016, pp. 1–7.

[102] S. Seo *et al.*, "HAMA: An efficient matrix computation with the MapReduce framework," in *Proc. IEEE 2nd Int. Conf. Cloud Comput. Technol. Sci.*, Nov. 2010, pp. 721–726.

[103] K. Siddique *et al.*, "Apache HAMA: An emerging bulk synchronous parallel computing framework for big data applications," *IEEE Access*, vol. 4, pp. 8879–8887, 2016.

[104] S. Chauhan, N. Agarwal, and A. K. Kar, "Addressing big data challenges in smart cities: A systematic literature review," *Info*, vol. 18, no. 4, pp. 73–90, 2016. [Online]. Available: https://doi.org/10.1108/info-03-2016-0012

[105] J. Wu, S. Guo, J. Li, and D. Zeng, "Big data meet green challenges: Big data toward green applications," *IEEE Syst. J.*, vol. 10, no. 3, pp. 888–900, Sep. 2016.

[106] M. Courtney, "Premium binds," *Eng. Technol.*, vol. 8, no. 6, p. 86, 2013.

[107] J. Wu, S. Guo, J. Li, and D. Zeng, "Big data meet green challenges: Greening big data," *IEEE Syst. J.*, vol. 10, no. 3, pp. 873–887, Sep. 2016.

[108] J. Wu, J. Thompson, H. Zhang, R. V. Prasad, and S. Guo, "Green communication and computing networks," *IEEE Commun. Mag.*, vol. 55, no. 11, pp. 12–13, Nov. 2017.

[109] J. Wu *et al.*, "Context-aware networking and communications: Part 1 [guest editorial]," *IEEE Commun. Mag.*, vol. 52, no. 6, pp. 14–15, Jun. 2014.

[110] R. Atat *et al.*, "Enabling cyber-physical communication in 5G cellular networks: Challenges, spatial spectrum sensing, and cyber-security," *IET Cyber Phys. Syst. Theory Appl.*, vol. 2, no. 1, pp. 49–54, Apr. 2017. [Online]. Available: http://digital-library.theiet.org/content/journals/10.1049/iet-cps.2017.0010

[111] (2017). *Why Anonymity Matters*. [Online]. Available: https://www.torproject.org/about/overview.html.en

[112] G. Suciu *et al.*, "Smart cities built on resilient cloud computing and secure Internet of Things," in *Proc. 19th Int. Conf. Control Syst. Comput. Sci.*, 2013, pp. 513–518.

[113] "2016 cost of data breach study: Global analysis," Ponemon Inst., Traverse City, MI, USA, Rep., 2016. [Online]. Available: http://www.ibm.com/security/data-breach

[114] A. Tiwari, "Big data: Securing the data," Geospatial World, Amsterdam, The Netherlands, Rep., 2013. [Online]. Available: https://www.geospatialworld.net/article/securing-the-data/

[115] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*. New York, NY, USA: Springer, 2006.

[116] D. Ferraiolo, J. Cugini, and D. R. Kuhn, "Role-based access control (RBAC): Features and motivations," in *Proc. 11th Annu. Comput. Security Appl. Conf.*, 1995, pp. 241–248.

[117] B. Ndibanje, H.-J. Lee, and S.-G. Lee, "Security analysis and improvements of authentication and access control in the Internet of Things," *Sensors*, vol. 14, no. 8, pp. 14786–14805, 2014. [Online]. Available: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4179010/

[118] N. Ye, Y. Zhu, R.-C. Wang, and Q.-M. Lin, "An efficient authentication and access control scheme for perception layer of Internet of Things," *Int. J. Appl. Math. Inf. Sci.*, vol. 8, no. 4, pp. 1617–1624, 2014.

[119] L. Gong, "A secure identity-based capability system," in *Proc. IEEE Symp. Security Privacy*, Oakland, CA, USA, 1989, pp. 56–63.

[120] P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "Identity driven capability based access control (ICAC) scheme for the Internet of Things," in *Proc. Int. Conf. Adv. Netw. Telecommun. Syst. (ANTS)*, 2012, pp. 49–54.

[121] P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "Identity establishment and capability based access control (IECAC) scheme for Internet of Things," in *Proc. 15th Int. Symp. Wireless Pers. Multimedia Commun.*, 2012, pp. 187–191.

[122] S. Gusmeroli, S. Piccione, and D. Rotondi, "A capability-based security approach to manage access control in the Internet of Things," *Math. Comput. Model.*, vol. 58, nos. 5–6, pp. 1189–1205, 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S089571771300054X

[123] J. L. Hernández-Ramos, A. J. Jara, L. Marín, and A. F. S. Gómez, "DCapBAC: Embedding authorization logic into smart things through ECC optimizations," *Int. J. Comput. Math.*, vol. 93, no. 2, pp. 345–366, 2016, doi: 10.1080/00207160.2014.915316.

[124] D. Crockford, "The application/json media type for javascript object notation (JSON)," Internet Eng. Task Force, Fremont, CA, USA, RFC 4627, 2006. [Online]. Available: http://www.ietf.org/rfc/rfc4627.txt

[125] L. Marin, A. Jara, and A. S. Gomez, "Shifting primes: Optimizing elliptic curve cryptography for 16-bit devices without hardware multiplier," *Math. Comput. Model.*, vol. 58, nos. 5–6, pp. 1155–1174, 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0895717713000563

[126] J. L. Hernández-Ramos, M. P. Pawlowski, A. J. Jara, A. F. Skarmeta, and L. Ladid, "Toward a lightweight authentication and authorization framework for smart objects," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 4, pp. 690–702, Apr. 2015.

[127] *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*," ANSI/IEEE Standard 802.11, 2003.

[128] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, "Extensible authentication protocol (EAP)," Internet Eng. Task Force, Fremont, CA, USA, Rep. RFC 3748, 2004.

[129] C. Rigney, S. Willens, A. C. Rubens, and W. A. Simpson, "Remote authentication dial in user service (RADIUS)," Internet Eng. Task Force, Fremont, CA, USA, RFC 2865, 2000. [Online]. Available: https://tools.ietf.org/html/rfc2865

[130] E. Rissanen, *Extensible Access Control Markup Language (XACML) Version 3.0*, OASIS Standard, vol. 22, 2013. [Online]. Available: http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html
[131] M. Egele, C. Kruegel, E. Kirda, and G. Vigna, "PiOS: Detecting privacy leaks in iOS applications," in *Proc. 18th Annu. Netw. Distrib. Syst. Security Symp.*, 2011, pp. 1–15.
[132] P. Gilbert, B.-G. Chun, L. P. Cox, and J. Jung, "Vision: Automated security validation of mobile apps at app markets," in *Proc. 2nd Int. Workshop Mobile Cloud Comput. Services*, Bethesda, MD, USA, 2011, pp. 21–26.
[133] W. Enck *et al.*, "TaintDroid: An information-flow tracking system for realtime privacy monitoring on smartphones," *ACM Trans. Comput. Syst.*, vol. 32, no. 2, pp. 1–29, 2014.
[134] W. Enck, M. Ongtang, and P. McDaniel, "Mitigating android software misuse before it happens," Netw. Security Res. Control, Dept. Comput. Sci. Eng., Pennsylvania State Univ., State College, PA, USA, Rep. NAS-TR-0094-2008, 2008.
[135] X. Xiao *et al.*, "User-aware privacy control via extended static-information-flow analysis," *Autom. Softw. Eng.*, vol. 22, no. 3, pp. 333–366, 2015, doi: 10.1007/s10515-014-0166-y.
[136] F. Roesner, "User-driven access control: A new model for granting permissions in modern operating systems," Qualifying Examination Project, Univ. Washington, Seattle, WA, USA, Rep., 2011.
[137] S. Chakrabarty and D. W. Engels, "A secure IoT architecture for smart cities," in *Proc. 13th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Las Vegas, NV, USA, 2016, pp. 812–813.
[138] X. Cao, X. Zeng, W. Kou, and L. Hu, "Identity-based anonymous remote authentication for value-added services in mobile networks," *IEEE Trans. Veh. Technol.*, vol. 58, no. 7, pp. 3508–3517, Sep. 2009.
[139] Z. Khan, Z. Pervez, and A. Ghafoor, "Towards cloud based smart cities data security and privacy management," in *Proc. 7th Int. Conf. Utility Cloud Comput.*, 2014, pp. 806–811.
[140] M. Strohbach, H. Ziekow, V. Gazis, and N. Akiva, "Towards a big data analytics framework for IoT and smart city applications," in *Modeling and Processing for Next-Generation Big-Data Technologies: With Applications and Case Studies*. Cham, Switzerland: Springer, 2015, pp. 257–282, doi: 10.1007/978-3-319-09177-8_11.
[141] D. Puiu *et al.*, "CityPulse: Large scale data analytics framework for smart cities," *IEEE Access*, vol. 4, pp. 1086–1108, 2016.
[142] Y. He *et al.*, "Big data analytics in mobile cellular networks," *IEEE Access*, vol. 4, pp. 1985–1996, 2016.
[143] Z. Li, S. Zhu, H. Hong, Y. Li, and A. E. Saddik, "City digital pulse: A cloud based heterogeneous data analysis platform," *Multimedia Tools Appl.*, vol. 76, no. 8, pp. 10893–10916, 2017, doi: 10.1007/s11042-016-4038-2.
[144] M. Sookhak, H. Talebian, E. Ahmed, A. Gani, and M. Khan, "A review on remote data auditing in single cloud server: Taxonomy and open issues," *J. Netw. Comput. Appl.*, vol. 43, pp. 121–141, Aug. 2014.
[145] M. Sookhak *et al.*, "Remote data auditing in cloud computing environments: A survey, taxonomy, and open issues," *ACM Comput. Surveys*, vol. 47, no. 4, 2015, Art. no. 65.
[146] C. Liu *et al.*, "Authorized public auditing of dynamic big data storage on cloud with efficient verifiable fine-grained updates," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 9, pp. 2234–2244, Sep. 2014.
[147] Q. A. Wang, C. Wang, K. Ren, W. J. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 5, pp. 847–859, May 2011.
[148] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 9, pp. 1717–1726, Sep. 2013.
[149] D. Estrin *et al.*, "Participatory sensing: Applications and architecture [Internet predictions]," *IEEE Internet Comput.*, vol. 14, no. 1, pp. 12–42, Jan./Feb. 2010.
[150] J.-P. Vasseur, G. Mermoud, and S. Dasgupta, "Mixed centralized/distributed algorithm for risk mitigation in sparsely connected networks," U.S. Patent EP2 954 649 A1, 2015. [Online]. Available: https://google.com/patents/EP2954649A1?cl=en
[151] Q. M. Ashraf and M. H. Habaebi, "Autonomic schemes for threat mitigation in Internet of Things," *J. Netw. Comput. Appl.*, vol. 49, pp. 112–127, Mar. 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804514002732
[152] N. C. Luong *et al.*, "Data collection and wireless communication in Internet of Things (IoT) using economic analysis and pricing models: A survey," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 4, pp. 2546–2590, 4th Quart., 2016.
[153] M. Sookhak *et al.*, "Fog vehicular computing: Augmentation of fog computing using vehicular cloud computing," *IEEE Veh. Technol. Mag.*, vol. 12, no. 3, pp. 55–64, Sep. 2017.
[154] "Phenonet: Distributed sensor network for phenomics supported by high resolution plant phenomics centre," CSIRO ICT Centre, CSIRO Sensor, and Sensor Networks TCP, Commonwealth Sci. Ind. Res. Organisation (CSIRO), Canberra, ACT, Australia, Rep., 2011.
[155] J. K. Zao *et al.*, "Augmented brain computer interaction based on fog computing and linked data," in *Proc. Int. Conf. Intell. Environ.*, Jun. 2014, pp. 374–377.
[156] C. Perera, Y. Qin, J. C. Estrella, S. Reiff-Marganiec, and A. V. Vasilakos, "Fog computing for sustainable smart cities: A survey," *ACM Comput. Surveys*, vol. 50, no. 3, pp. 1–32, Jun. 2017.
[157] M. Sookhak, R. Yu, and A. Y. Zomaya, "Auditing big data storage in cloud computing using divide and conquer tables," *IEEE Trans. Parallel Distrib. Syst.*, vol. 29, no. 5, pp. 999–1012, May 2018.
[158] P. Zhang *et al.*, "A survey on access control in fog computing," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 144–149, Feb. 2018.
[159] S. Khan, S. Parkinson, and Y. Qin, "Fog computing security: A review of current applications and security solutions," *J. Cloud Comput. Adv. Syst.*, vol. 6, no. 19, pp. 1–22, 2017.
[160] J. New, D. Castro, and M. Beckwith, "How national governments can help smart cities succeed," Center Data Innovat., Washington, DC, USA, Rep., 2017. [Online]. Available: http://www2.datainnovation.org/2017-national-governments-smart-cities.pdf
[161] E. Hamilton. (2016). *Smart Cities Require Smart Policy*. [Online]. Available: https://www.usnews.com/opinion/economic-intelligence/articles/2016-11-07/smart-cities-must-balance-privacy-with-government-transparency

Mehdi Sookhak was a Post-Doctoral Fellow with Carleton University, Canada, funded by Canadian Natural Sciences and Engineering Research Council. He is a Lecturer with the Polytechnic School, Arizona State University. He was an Active Researcher with the Center of Mobile Cloud Computing Research, Faculty of Computer Science and Information Technology, University Malaya, Kuala Lumpur. His areas of interest include cryptography and information security, mobile cloud computing, computation outsourcing, access control, wireless sensor and mobile ad hoc networks (architectures, protocols, security, and algorithms), and distributed systems.

Helen Tang received the Ph.D. degree in electrical engineering from Carleton University in 2005. She is the Portfolio Manager of Cyber Electromagnetics with the Center for Security Science, Defence Research and Development Canada, Ottawa. From 1999 to 2005, she had worked in several research and development organizations in Canada and USA, including Alcatel-Lucent, Mentor Graphics, and Communications Research Center Canada. From 2005 to 2015, she was a Defence Scientist with DRDC-Ottawa. She has been involved in many projects related to cyber security. She is also an Adjunct Professor with the Department of System and Computer Engineering, Carleton University, where she is the supervisor of several graduate students. She was a recipient of the Outstanding Contribution Award at DRDC Ottawa in 2009 and 2016, the Best Paper Award at IEEE/IFIP TrustCom 2009, and the Outstanding Leadership Award at IEEE/IFIP TrustCom 2010.

Ying He (S'16) received the B.S. degree in communication and information systems from Dalian Ocean University, Dalian, China, in 2011 and the M.S. degree in communication and information systems from the Dalian University of Technology, Dalian, in 2015. She is currently pursuing the Ph.D. degree with the Department of Systems and Computer Engineering, Carleton University, Canada. Her current research interests include wireless systems, security, big data, and machine learning.

F. Richard Yu (S'00–M'04–SM'08–F'18) received the Ph.D. degree in electrical engineering from the University of British Columbia in 2003. From 2002 to 2006, he was with Ericsson, Lund, Sweden, and a start-up in California, USA. He joined Carleton University in 2007, where he is currently a Professor. His research interests include wireless cyber-physical systems, connected/autonomous vehicles, security, distributed ledger technology, and deep learning. He was a recipient of the IEEE Outstanding Service Award in 2016, IEEE Outstanding Leadership Award in 2013, Carleton Research Achievement Award in 2012, the Ontario Early Researcher Award (formerly, Premiers Research Excellence Award) in 2011, the Excellent Contribution Award at IEEE/IFIP TrustCom 2010, the Leadership Opportunity Fund Award from Canada Foundation of Innovation in 2009, and the Best Paper Awards at IEEE VTC 2017 Spring, ICC 2014, Globecom 2012, IEEE/IFIP TrustCom 2009, and International Conference on Networking in 2005.

He serves on the editorial board of several journals, including the Co-Editor-in-Chief for *Ad Hoc and Sensor Wireless Networks*, a Lead Series Editor for the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, the IEEE TRANSACTIONS ON GREEN COMMUNICATIONS AND NETWORKING, and the IEEE COMMUNICATIONS SURVEYS AND TUTORIALS. He has served as the technical program committee co-chair of numerous conferences. He is a Registered Professional Engineer in the province of Ontario, Canada, and a fellow of the Institution of Engineering and Technology. He is a Distinguished Lecturer, the Vice President (Membership), and an Elected Member of the Board of Governors of the IEEE Vehicular Technology Society.