Received: 13 March 2019 | Revised: 13 May 2019 | Accepted: 5 June 2019

DOI: 10.1002/ett.3677

SPECIAL ISSUE ARTICLE

WILEY

An overview of security and privacy in smart cities' IoT communications

Fadi Al-Turjman[1] | **Hadi Zahmatkesh**[2] | **Ramiz Shahroze**[1]

[1] Department of Computer Engineering, Antalya Bilim University, Antalya, Turkey

[2] Computer Engineering, Middle East Technical University, Northern Cyprus Campus, Guzelyurt, Mersin, Turkey

Correspondence
Hadi Zahmatkesh, Computer Engineering, Middle East Technical University, Northern Cyprus Campus, 99738, Guzelyurt, Mersin 10, Turkey.
Email: zhadi@metu.edu.tr

Abstract

Smart cities have brought significant improvements in quality of life and services to citizens and urban environments. They are fully enabled to control the physical objects in real time and provide intelligent information to citizens in terms of transport, healthcare, smart buildings, public safety, smart parking, and traffic system and smart agriculture, and so on. The applications of smart cities are able to collect sensitive information. However, various security and privacy issues may arise at different levels of the architecture. Therefore, it is important to be aware of these security and privacy issues while designing and implementing the applications. This paper highlights main applications of smart cities and addresses the major privacy and security issues in the architecture of the smart cities' applications. It also reviews some of the current solutions regarding the security and privacy of information-centric smart cities' applications and presents future research challenges that still need to be considered for performance improvement.

1 | INTRODUCTION

In recent decades, the population of urban areas is rapidly increasing. Based on a report from the United Nations Population Fund, more than 50% of population in the world inhabit urban environments.[1] The concept of "smart city"[2] has attracted too much attention by both academia and industry due to its strong requirements and practical background in an urbanized environment. Several cities have begun to develop their own strategies toward the concept of smart cities to enhance the quality of life and provide better services to citizens.

Many countries with growing population are spending a vast amount of money on smart cities-related projects. For example, China is working on more than 200 projects toward smart cities paradigm.[3] Smart cities-related technologies are enabling the urban municipals to manage their everyday operations to make people's life easier. Smart cities' infrastructure includes many devices and interconnected systems to benefit people in a variety of applications such as smart healthcare, smart transportation, smart parking, smart traffic system, smart agriculture, and smart homes to just name a few.

Information-centric networking (ICN) is a networking paradigm, which is able to maintain packet delivery in unreliable environments. Therefore, ICN can be considered as an alternative for the IP-based networks in smart cities.[4]

The integration of various low-cost smart devices such as sensors and actuators, and the rapid development of wireless communication technologies enabling small and low-cost objects to connect to the internet has resulted in the rise in the deployment of Internet of Things (IoT) where physical objects are changing to smart objects in everyday life. Besides IP-based approaches such as the one presented in the work of Sheng et al,[5] ICN solutions can be applied to develop the emergence of IoT and its related applications. Information-centric networking is characterized as a concept to name content and locate information at the center of the architecture[6] rather than depending on the IP host identifiers.

The principal idea is to completely change the internet to a more generic and simpler architecture.[7] ICN can support various IoT scenarios and overcome their current limitations by utilizing its advantages to deploy various applications in heterogeneous environments such as smart homes and smart cities.[8] It can also be used as a framework to connect different objects with sensing capabilities to provide multiple services in the IoT environments. Moreover, the use of ICN can reduce the energy consumption in the IoT era.[9]

Cities are being smart and this may cause people to face huge security and privacy risks.[10] This is because of the nature of resource-constrained devices, which makes the smart city vulnerable to different security attacks.[11] These vulnerabilities may cause several cyberattacks in smart cities. For instance, malicious attackers may produce false data during the manipulation of sensing data, which results in the loss of control over the highly intelligent systems.[10] In 2015, 230 000 people in Ukraine suffered a major breakdown of electricity due to the attack of hackers to the smart grid (SG), which happened to the people in the form of denial-of-service (DoS) attack.[1] Many resource-constrained devices such sensors and cameras, which are collecting and sharing sensitive data in smart cities, can also be vulnerable to attacks by the malicious hackers threatening the security and privacy of people in smart cities. Due to these cyberattacks, home area information that is collected and controlled through smart homes can provide a way to reveal people's lifestyle in terms of privacy and even result in economic loss.[10]

According to a report, the market of smart cities is expected to gradually increase to $1.5 trillion by 2020.[12] Actually, governments are responsible to attract large investments to fulfill the vision of smart cities.[13] This huge improvement includes deployment of thousands of sensor nodes in the city to provide real-time information to people about different services such as public transportation, traffic flows, the quality of water and air, and the energy consumption rate, to just name a few.[14] However, processing and analyzing the vast amount of sensitive data generate a number of security and privacy challenges and concerns regarding how to protect the sensitive data in the presence of unauthorized parties.[10,15]

In the IoT era and smart cities, cloud computing can provide cost-effective services for data processing and storage. However, there are some issues in cloud-based IoT applications such as lack of mobility support, location awareness, latency, and security, which can be resolved by fog computing paradigm.[16,17] Fog computing addresses these challenges by providing computing services to the users at the edge of the network, which, in turn, reduces latency and enhances the quality of service.[18] However, security and privacy are challenging issues in fog computing due to the differences in fog computing and cloud computing which make the security solutions for cloud services not suitable for fog computing services available to the users. Various cryptographic techniques can deal with security attacks. However, these techniques are not appropriate for resource-constraint IoT devices in smart cities. One solution in this regard can be offloading additional operations related to security to a fog-based node, which can enable security and data analysis directly at the edge of the network.[19] In addition, in publish and subscribe systems, which spread data from publisher to subscriber, publication is disseminated using a set of brokers, which can collect sensitive information of the users. In this regard, the system must ensure confidentiality of the publications and subscriptions while brokers are trying to have access to publications' tags and interests of subscribers.[20]

According to a definition by IBM, the concept of smart city is based on three main characteristics called "instrumented," "interconnected," and "intelligent,"[21] which are shown in Figure 1.

Instrumented: This characteristic means a city, which is covered with a group of devices such as sensors and actuators. Therefore, the core systems of the cities have access to reliable and real-time information using these devices.

Interconnected: It means that smart city has a huge set of systems that are cooperating to provide information from various locations and sources. It is then possible to create a link from the physical world to the real world by using an accurate combination of interconnected and instrumented systems.

Intelligent: It refers to an instrumented and interconnected environment that utilizes the information obtained from various systems and devices such as sensors to improve the quality of life of the citizens.

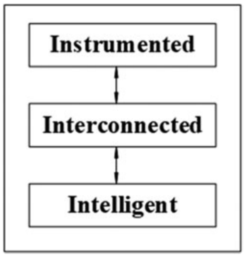

FIGURE 1 Main characteristics of smart cities

1.1 | Comparison to similar surveys

In spite of the aforementioned benefits of smart cities, several security and privacy concerns are arising due to the large number of wirelessly connected sensors and cameras which are collecting and sending data to base stations and other internet devices used to process data. All these devices are generating sensitive data over different networks. Data is the most precious asset of people in today's smart world. All data is handled by software and hardware that have some security and privacy issues such as the vulnerabilities in infrastructures, and cyberattacks (eg, DoS attacks). Due to these security issues, the performance of highly innovative systems can degrade in the form of services. It is important to overcome these security challenges to make the future of the highly advanced system more secure and beneficial for the users.[22]

There are several published survey papers related to the security and privacy of IoT and smart cities. For example, in the work of Zhang et al,[10] security and privacy in smart cities' promising applications were investigated. The authors also discussed several security and privacy challenges in these applications. In the work of Gharaibeh et al,[23] the authors identified the techniques used for data security and privacy and discussed the technologies that make smart cities a reality. The study in the work of Eckhoff and Wagner[24] discussed different privacy types, attackers, and the required sources for the attacks in smart cities. The authors also reviewed the current privacy-improving techniques and various types of citizens' privacy in smart cities. Similarly, the main research challenges and the current security solutions in the IoT environments were presented in the work of Sicari et al.[25]

Our contributions in this study relative to the recent literature can be summarized as follows.

- This paper highlights main applications of smart cities and addresses the major privacy and security issues in the architecture of the smart cities' applications.
- We provide a number of solutions to deal with critical threats regarding the security and privacy in smart environments.
- We also propose a secure IoT architecture for the smart cities.
- Security and privacy techniques dealing with the process of developing secure systems are also discussed in the manuscript.
- Finally, we provide some open research issues and challenges that should be taken into account regarding the improvements of the smart cities in terms of security and privacy.

The remainder of this article is organized as follows. Section 2 presents an IoT-based architecture that focuses on the security and privacy issues in smart cities. Some typical applications of smart cities are outlined in Section 3. Sections 4 and 5 discuss a number of security and privacy issues and solutions in smart cities' environment, respectively. The general requirements regarding the security and privacy challenges for smart cities' services are presented in Section 6. Section 7 proposes a secure IoT-based architecture for smart cities. Section 8 discusses some open research issues and provides future research directions. Finally, Section 9 concludes this paper. A list of abbreviations together with their brief definitions used throughout the paper is provided in Table 1 to help the readers in understanding the abbreviated terms.

2 | ARCHITECTURE OF SMART CITIES

In this section, we provide an IoT-based architecture that emphasizes on the security and privacy issues in smart cities. This architecture is built upon the architecture proposed in[26] and is shown in Figure 2. A brief discussion of each layer of the architecture is provided in the following sections.

2.1 | Physical layer

Physical layer is also known as perception layer or lower layer of the architecture. This layer contains heterogeneous devices (eg, sensors and actuators) that collect information and send it to the upper layer of the architecture called network layer for further processing.

2.2 | Network layer

Network layer is also known as communication layer, which is the core layer of the IoT-based architecture. This layer is dependent on basic networks such as wireless sensor networks (WSNs) and the internet, and communication networks. The main responsibility of the network layer is to transmit the collected data by the physical layer and to connect together various devices of the network such as servers and smart things.

TABLE 1 List of abbreviations

Abbreviated	Name
6LoWPAN	IPv6 over low-power wireless personal area networks
AA	Availability attack
AI	Artificial intelligence
AS	Autonomous system
AV	Autonomous vehicle
BLE	Bluetooth low energy
BN	Black network
BS	Base station
CA	Content analysis
CCTV	Closed-circuit television
CoAP	Constrained application protocol
CS	Crowed sensing
DDoS	Distributed denial of service
DoS	Denial of service
EVC	Electronic vehicles charging
FI	False information
GPS	Global positioning system
HAI	Home area information
HE	Homomorphic encryption
HetNet	Heterogeneous network
HTTP	Hypertext transfer protocol
ICN	Information-centric network
ICT	Information and communication technology
IDS	Intrusion detection system
IHS	Intelligent healthcare system
IoT	Internet of Things
IS	Identity spoofing
ITS	Intelligent transport system
KMS	Key management system
LTE	Long-Term Evolution
MCS	Mobile crowd sensing
ML	Machine learning
M2M	Machine to machine
MM	Message modification
MQTT	Message queuing telemetry transport
P2P	Peer to peer
PPBS	Privacy-preserving biometric scheme
PPDM	Privacy-preserving data mining
QoS	Quality of service
RFID	Radio frequency identification
SDN	Software-defined networking
SG	Smart grid
SSL	Secure sockets layer
TA	Traffic analysis
TTP	Trusted third party
UAV	Unmanned aerial vehicle
UDP	User datagram protocol
UN	United Nations
UR	Unified registry
VoIP	Voice over IP
WSN	Wireless sensor network

2.3 | Database layer

Database layer is also known as support layer and it operates closely with the upper layers of the architecture. It consists of database servers and intelligent computing systems. The main responsibility of this layer is to provide support for application requirements through intelligent computing approaches such as cloud/edge computing.

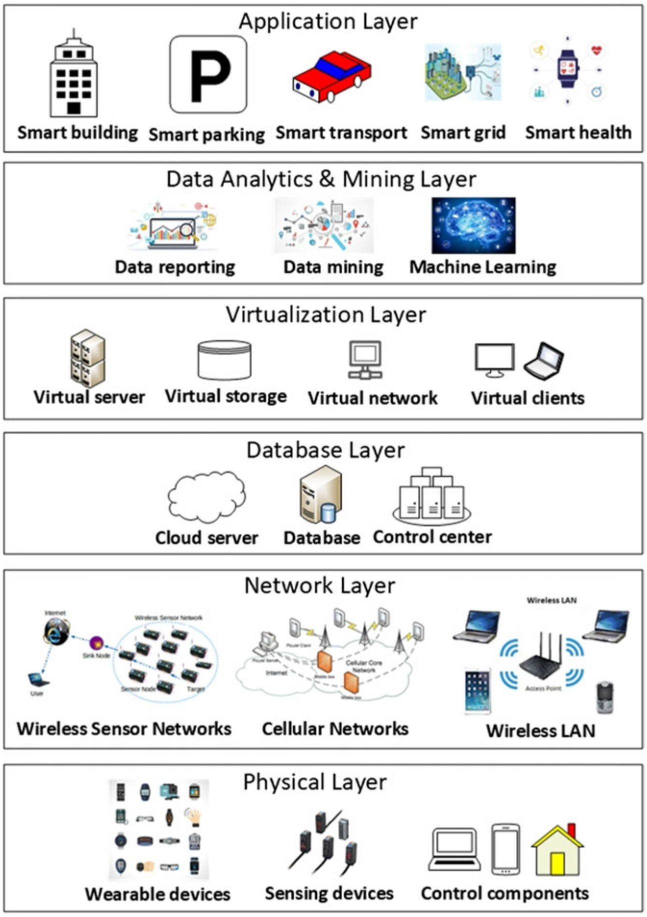

FIGURE 2 An overview of the Internet of Things–based architecture for smart cities

2.4 | Virtualization layer

This layer provides a mechanism called virtual network to integrate hardware/software and network functionality into a single software-based entity that is configured logically. A network virtualization[27] may need platform virtualization together with resource virtualization to be successful. This is obtained using the virtualization layer.

2.5 | Data analytics and mining layer

In data analytics and mining layer, raw data is converted into valuable information, which can help improve the efficiency of the network and predict the future events such as failure in the system. This layer employs various data mining and data analytics techniques such as machine learning (ML) algorithms to analyze the data.

2.6 | Application layer

This is the top layer of the secure IoT-based architecture and is responsible to provide intelligent and smart applications and services to the users based on their individual requirements. Some typical ones of these applications are briefly described in the following section.

3 | APPLICATIONS OF SMART CITIES

Various applications of smart cities have been emerged to monitor the physical world. These applications are able to sense and collect information through thousands of smart devices (eg, sensors) via internet to make people's lives much easier and effective in different aspects like environment, energy, transportation, safety, healthcare, parking, and traffic systems. In the following sections, we describe some typical ones on these applications.

3.1 | Smart grid

Smart grid is the next generation of the electric grid and has been often used to refer to applications of power grid such as the peer-to-peer (energy trading.[28] Smart grid is a data communication network, which provides a smart approach to integrate conventional power generation, energy storage, transmission and distribution, and demand management to enhance reliability and provide higher operational efficiency and better power quality.[29] Smart grid is an intelligent monitoring system that control the electricity flowing via the grid system. This uses devices that have the capability of bidirectional communication to measure and sense production and consumption of electricity. It then sends the information to the operators and users and automated devices for monitoring and making decision regarding any changes in the condition of the electricity grid.[30]

3.2 | Smart transportation

The aim of smart or intelligent transportation is to provide a smarter use of transport system such as the infrastructure for electronic vehicles charging.[31,32] Smart transportation consists of intelligent networks that can serve people by improving safety, reliability, and speed.[33] By using smart applications such as transport-oriented smartphones, people can easily search the fastest and the most economic routes, schedule their visits, and easily find the location of buses and trains. Smart transportation also facilitates car-parking searching and license recognition systems.[34]

3.3 | Smart environment

Smart environment can have significant contribution toward the building of sustainable societies for smart cities. By using technical management devices, smart cities are able to monitor air quality, traffic congestion, and energy consumption, and to enhance waste and pollution efficiency.[35] Moreover, smart environment can monitor greenhouse gases, forest condition, city noise, etc, to entail the sustainable and intelligent development. It may also be possible to forecast and discover disasters in the future by using environmental WSNs.[36]

3.4 | Smart living

Smart living provides intelligent management of different home appliances to enhance energy efficiency and provide convenient home.[37] It can also support remote monitoring of home appliances, energy savings, education, and entertainment. In addition, the applications of smart living can also manage the process of waste recycling and parking to provide a smart building with convenient life and great experience and sustainable energy and environments for the residents.[10]

3.5 | Smart health

In smart cities, the concept of smart health is to provide the health services by using networks and sensing infrastructures of smart cities.[38] Intelligent healthcare system (IHS) provides health monitoring and proper diagnosis to the people in smart cities.[39] The health conditions of the people can be timely monitored by using medical sensors and wearable devices.[40] The health data can then be forwarded to the processing unit for further diagnosis of the doctors. Moreover, the complete health-related information of the patients can easily be accessed through a database, which, in turn, increases the possibility of diagnosing infectious or chronic illnesses in the early stage.[10]

3.6 | Smart energy

In smart cities, sensor nodes are widely deployed to monitor energy generation and consumption. In this regard, smart energy[41] leveraging SG and electronic vehicles charging can reduce the energy consumption and stop the failure of the electricity supply in power grid and individual energy usage.[10]

4 | SECURITY AND PRIVACY ISSUES IN SMART CITIES' APPLICATIONS

Recently, significant problems have been occurred in various application scenarios. For instance, in SGs, the smart metering infrastructure can control the private lives of the citizens such as their working hours in smart cities.[42] Furthermore, in smart homes and healthcare context, service providers and device manufacturers can have access to sensitive information of the users.[43] Moreover, smart mobility applications can collect huge amount of information related to trajectory of a user, which can be used to predict the mobility pattern and location of the user.[44] In addition to these problems, security and privacy have become a major challenge in smart cities-related applications since cities are focusing to become smarter. In recent decades, several security and privacy issues have been found in various smart cities–related applications.[1] In the following sections, we list and briefly discuss some majors ones of these security issues.

4.1 | Cyber security

Cyberattacks compromise security of smart cities' applications and are mainly of two types: active attack and passive attack. The aim of passive attack is to learn and use different information of the system without any changes in resources of the system. The main target of this attack is "transmitted information" for the purpose of learning the configuration and behavior of the system and its architecture. It is hard to detect these attacks because the data is not modified. That is why it is better to focus more on the prevention of such attacks. On the other hand, the active attacks are scheduled to produce an effect or change in the operation of the system using data modification or adding incorrect data into the system. Sabotage, manipulation, and espionage are the main reasons behind cyberattacks.[45] The main cyberattacks, which may occur in various smart cities' application, are briefly described in this section as follows.[46]

Denial of service: Denial of service can also be called "availability attack." The main purpose of DoS attack is to suspend the communication of the system. To do so, attacker can disable the physical components access through the excessive messages on the communication network, which prevents the normal operation of the system. The DoS attacks are a type of attacks, which can destroy the availability of the targeted system in smart cities. This type of attacks can be classified into network layer and application layer DoS attacks.[47] Network layer DoS attacks are performed at the network layer and they try to overwhelm the resources of the network of the targeted system with bandwidth consuming attacks such as user datagram protocol flooding attacks. The application layer DoS attacks, on the other hand, utilizes the special characteristics of the application layer protocols such as hypertext transfer protocol and voice over IP to affect on the resources.[48] In smart cities, the impacts of both types of DoS attacks on any system that provides centralized monitoring in these areas can be extremely bad since the unavailability of the system would result in total chaos in the cities.[49]

Malware: This is a malicious software that can gain illegal access to the system. It can also use internal weaknesses of the system aiming to steal, change, and ruin physical system components and related information. For example, smart cities may contain several closed-circuit television cameras controlled either privately or by public authorities. The security of these cameras is a challenging task as some of them lack encryption algorithms and others are vulnerable to attack by malware.[50] Accessing a camera can provide a way to view individual's homes or use a bank camera to control and view the digits being pressed by the users.

Eavesdropping: This is an instance of a passive attack, which is defined as an illegal listening to a communication without the permission of the communication's parties. Eavesdropping is a dangerous attack in smart cities that results in break down the confidentiality and integrity of the network and can lead to personal and financial failures.[51] It can be used to spy on communication channels to capture the behavior of the network traffic and obtain the network map.

Masquerading: It is also known as "impersonation" or "identity spoofing." In masquerading, the attacker tries to steal information by pretending to be a legal device or entity. For example, in intelligent transport system (ITS) as an application of smart cities, masquerading can provide unauthorized access to restricted information, which may ruin the integrity of the network. It may also result is loss, corruption, and manipulation of information in ITS.[52]

False information (FI): Attackers transmit erroneous amount of FI in the network, which might affect the behavior of other drivers. It can be both intentional and unintentional. Introducing FI on the systems in smart cities may result in delays and unnecessary congestions as people act based on the FI provided to them.

Message modification: In this attack, the message is modified to make an unexpected behavior happens in the system. Message modification may also include reordering a stream of message and/or message delay. Similar to FI, message modification can cause unnecessary congestions and delays in the systems and threaten data integrity. As a result, threat to data integrity may harm people and infrastructures of smart cities.[53]

Traffic analysis (TA): Traffic analysis is similar to eavesdropping but here, rather than content analysis, attackers monitor the traffic pattern and obtain useful information from it. Combining TA with eavesdropping may damage privacy. In addition, obtaining illegal information from TA attacks can harm confidentiality of information in smart cities.

Summary of the cybersecurity attacks, which may occur in smart cities, is presented in Figure 3.

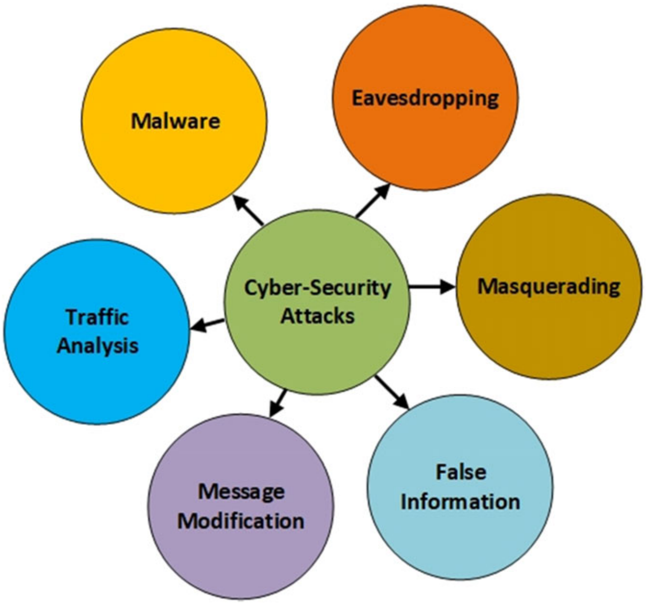

FIGURE 3 Summary of the cybersecurity attacks in smart cities

4.2 | Botnet activities in IoT-based smart cities

Botnets are one of the latest issues which have recently posed serious risks to IoT-based systems. An example of such botnets would be Mirai botnet, which modifies or destroys information on various devices such as routers, webcams, IP cameras, and printers and send the infection to various IoT devices. This may finally result in a distributed DoS attack against the target servers.[54] The IoT devices are usually designed with almost no security compared to other smart devices such as smart phones and computers. This danger was not recognized until 2016; therefore, more research is required to overcome this threat in the future. Otherwise, this attack will damage the IoT ecosystem.[55] An approach to prevent such attacks was presented in the work of Ghafir et al.[56] The authors proposed an approach called BotDet for botnet command and control traffic detection to protect critical systems against malware attacks. They developed four detection modules to discover various techniques utilized in botnet command/control communications and designed a system for alert correlation according to the voting between the detection modules. The results reveal the capability of real-time detection in the approach and show that the proposed system balances the false- and true-positive rates with more that 13% and 82%, respectively.

4.3 | Threats of unmanned autonomous vehicles in smart cities

Driverless cars or autonomous vehicles are a type of car that drive itself without the human involvement using various in-vehicle technologies and devices such as sensors, global positioning system and antilock braking system, etc. Autonomous vehicles have gained too much attention toward the building of a smarter society with the goal of reducing the ratio of traffic accidents. Despite all the benefits of this growing application, there are major security and privacy risks once it is hacked, because it will then threaten data privacy and life safety of the citizens in smart cities.[57] Particularly, hackers can use the security bugs to control the vehicle to shut down the engine or apply the brakes in various situations. Moreover, the huge amount of personal data obtained from the computer system of an autonomous vehicle may cause crucial security and privacy issues.

4.4 | Privacy leakage

Attackers can collect, transmit, and process private information such as health conditions, identity and location of the users in transportation context, and lifestyle derived from the intelligent surveillance systems. This, in turn, makes the smart cities vulnerable to privacy leakage. To overcome this issue, a number of security and privacy solutions (eg, anonymity, access control, and encryption) can be employed to save sensitive information in smart cities against the attacks of hackers.[58,59] However, most of the existing security and privacy techniques are designed only against outside attackers and do not consider the role of potential inside attackers.[59] For example, a smart building may use a surveillance camera to discover robbery or unusual activities. Attackers from inside the building (eg, employees or those who have access the surveillance records) may steal private data or provide a gap for attackers outside the building. Therefore, it is a challenging task to develop a security and privacy mechanism in smart cities to have a balance between privacy and efficiency.

5 | SECURITY AND PRIVACY SOLUTIONS FOR SMART CITIES' ENVIRONMENT

In this section, a number of security and privacy solutions are introduced which are utilized to deal with critical threats regarding the security and privacy in smart environments.

5.1 | Blockchain

Blockchain is a peer-to-peer distributed, centralized, and public decentralized technique that is used to store transactions, sales, agreements, and contracts across many computers.[11] Blockchain is basically a chain of blocks, where digital information is stored in a public database. It is specially developed for cryptocurrency such as bitcoin and litecoin. Blockchain technology has gained more attraction in recent years. The comprehensive survey in the work of Christidis and Devetsikiotis[60] verified the reliability of utilizing this technology in IoT environments and reveals its significance in the developing IoT ecosystems. The main reason behind the success and importance of blockchain technology in IoT applications is its decentralized feature, which enables various applications to work in a distributed manner. For instance, in the work of Biswas and Muthukkumarasamy,[11] the authors proposed a security framework based on the blockchain technology that can secure the communication of different devices in smart cities and enhance the effectiveness and reliability of the system. Moreover, a new security framework is developed by the integration of blockchain technology into a smart home to improve integrity, confidentiality, and availability.[61] Similarly, security and privacy issues in vehicular communications were addressed using blockchain technology in the work of Lei et al.[62] In the work of Zyskind et al,[63] the authors proposed a personal data management system that integrates blockchain technology with off-blockchain storage solution so that the users are aware of the collected data by the providers. Fu et al[64] proposed an auditing system based on blockchain for shared data in cloud-based applications. They presented an approach where a number of entities should collaborate to get back the identity of a malicious user. Based on the proposed blockchain-based architecture, data changes can be traced and correct data blocks can be recovered when the data are damaged. In addition, various design requirements of solutions based on blockchain technology for data origin tracking were discussed in the work of Neisse et al.[65] The authors presented the assessment of their implementation results to provide a complete overview of various specified approaches. In the work of Laurent et al,[66] a blockchain-based access control was presented that allows owners of data to specify access rights for the data sources on remote servers and change the privileges when required. This approach provides an authenticated access control managed by blockchain technology that ensures the preservation of users' privacy. Furthermore, blockchain technology can provide robust solutions and secure smart cities from cyberattacks. For example, blockchain-based digital smart ID can be assigned to everyone and everything to provide authentication and authorization for people and connected devices within smart cities' network.

5.2 | Cryptography

Algorithms utilizing cryptography techniques are the backbone of the security and privacy protection in information-centric smart cities' applications since they prevent the access of unauthorized parties during the data storing, transmitting and processing. The existing cryptographic tools utilized in smart cities' applications are discussed in this section. Traditional encryption algorithms and standards are not fully appropriate for resource-constrained smart devices due to the energy consumption and computational complexity.[67] Therefore, it is a basic requirement to use lightweight encryption for utilizing cryptographic algorithms in practice. For instance, in the work of Mahmood et al,[68] the authors proposed a mechanism for IoT-based scenarios that can secure end-to-end communications of the users from distributed DoS attacks. Moreover, a lightweight authentication protocol was developed in the work of Li et al[69] to secure smart cities' applications by using a public key encryption strategy. In addition, homomorphic encryption has recently attracted too much attention due to its strength and capability on computations of encrypted data. For instance, homomorphic encryption can be utilized for the protection of electricity consumption in SG systems[70] and for solving security and privacy issues in cloud computing.[71] It can also be used to protect security and privacy in healthcare monitoring systems.[72] Moreover, cryptography approaches can be considered as one of the most convenient and effective techniques to provide security for cloud-based data as they significantly improve the security and privacy of data particularly in public cloud environment.[73] In addition, cryptographic techniques support well-known privacy preservation algorithms and are able to offer very precise analysis results.[73] However, it may also be possible to attack cryptographic algorithms with the help of simple power analysis. Attackers may control and change the data by intentionally injecting errors trying to have an effect on the performance of the device.[74] Therefore, it is important to carefully conduct research in cryptographic algorithms to ensure the security and privacy of the data. In addition, cryptography can be used to solve the problem of privacy leakage caused by public access policy.[75] For example, Cui et al[76] proposed a scheme to consider a tradeoff between decryption possibility and the policy privacy in which the attribute information in the policy is divided into two parts, ie, value and name. In the proposed method, the value attribute is hided in the access policy instead of concealing the whole attribute. Therefore, it can protect the policy privacy reasonably.

5.3 | Biometrics

Biometrics are broadly used for authentication in IoT-based infrastructures. This technology widely depends on human behavior and automatically recognizes a person through bio-data obtained from faces, fingerprints, handwritten signatures, voices, etc. One of the most accurate methods, which can obtain high accuracy and efficiency, is brainwave-based authentication.[77] Similarly, a mutual authentication protocol was proposed in the work of Amin et al[78] to keep safe the private information of the users in storage devices. Please note that the risk of privacy leakage would increase if the mentioned bio-based approaches are not used properly. For example, in the work of Natgunanathan et al,[79] the authors reported that it is required to develop privacy-preserving biometric schemes similar to the one presented in the work of Wang et al.[80] Moreover, they revealed that these biometrics have promising use-cases in the future in various applications such as e-business. Biometrics can also be used to encrypt communication between an unmanned aerial vehicle (UAV) and a base station. For example, the study in the work of Singandhupe et al[81] proposed a safety mechanism with low-cost resources based on biometrics for the UAV if an attack is detected. The authors showed that the proposed approach could be applied to any UAV scenario where the cybersecurity attacks are an important issue.

5.4 | Machine learning and data mining

Machine learning is a part of artificial intelligence with the goal of developing systems, which are able to learn from past experience. According to the current situations, ML techniques can be used to enhance the efficiency of intrusion detection systems in IoT environments.[1] For example, the study in the work of Alsheikh et al[82] showed the advantages of using ML technologies to provide security in WSNs. Similarly, Luo et al[83] developed a machine-based approach to improve security of data sensing in WSNs. In addition, a novel model utilizing ML algorithms was developed in the work of Aminato et al[84] to discover attacks in Wi-Fi networks. There are also several studies that employed ML technologies to strengthen defense-related strategies. For instance, in the work of Shamshirband et al,[85] the authors developed a model based on game theory and ML technologies to discover and prevent intrusions in WSNs. Moreover, the existing studies on biometric security systems from the ML point of view was reviewed in the work of Biggio et al.[86] In addition, there are different ML techniques such as supervised learning and unsupervised leaning that can be applied to effectively detect the presence of a botnet.[87] However, there are still some issues such as real-time monitoring and adaptability to new attacks that need to be solved regarding ML-based detection techniques.

Data mining is another technique that can be applied to handle security and privacy in smart cities environments. Tsai et al[88] showed that the huge amount of data collected by various sensors in smart cities are utilized to mine new information and regulations which in turn provides better services to the users. However, using data mining techniques may result in some security and privacy concerns regarding the disclosure of sensitive information of the users such as their locations. In this regard, privacy-preserving data mining techniques can be applied to overcome this problem.[89,90]

5.5 | Internet of Things regulations

Internet of Things includes a wide range of communication technologies such as machine-to-machine communication, sensors, wireless communication, and radio frequency identification. However, the IoT industry is still not regulated. This has resulted in broader security and privacy implications. The use of unsecured smart devices in various industries such as military and health, and the fact that IoT devices can be easily hacked has created new attacks, which can happen at each layer of the IoT protocol stack.[91] While the IoT industry has been aware of the issues related to security and privacy, recent cyberattacks on IoT devices such as the one presented in the work of Jerkins[92] and other similar attacks had unintended

Ref	Blockchain	Cryptography	Biometrics	ML
Zhang et al[10] and Eckhoff and Wagner[24]	-	X	X	-
Elmaghraby and Losavio[59] and Dorri et al[61]	X	-	-	-
Mahmood et al[68] and Li et al[69]	-	X	-	-
Natgunanathan et al[79] and Wang et al[80]	-	-	X	-
Gharaibeh et al[23]	X	X	-	X
Alsheikh et al[82] and Luo et al[83]	-	-	-	X
Christidis and Devetsikiotis[60] and Lei et al[62]	X	-	-	-
Sicari et al[25]	-	X	X	-
Aminanto et al[84] and Shamshirband et al[85]	-	-	-	X

ML = Machine Learning
X = Considered, − = Not considered.

TABLE 2 A summary of the security and privacy solutions in smart cities' environments

results of increasing the awareness[93] regarding the needs of having strong security mechanisms and regulations for the devices that are connected to the internet.

A Summary of the aforementioned solutions for smart cities' environments is presented in Table 2.

6 | SECURITY AND PRIVACY REQUIREMENTS FOR SMART CITIES' SERVICES

In this section, we briefly discuss security and privacy techniques dealing with the process of developing secure systems.

6.1 | Privacy by design

This is a strategy trying to fix the security and privacy issues in information-centric smart cities.[94] This strategy includes some principles that should be taken into account while designing a new system.[95] For example, there should be a proactive privacy protection rather than a post reaction after happening the violations. Moreover, privacy should be considered in the design of the system and available as the default setting. In addition, there should be protection for the whole lifecycle of the data. Finally, the system should have transparency and visibility, and respect the user privacy. Several studies utilized these principles in developing new privacy-friendly systems. For instance, the study in the work of Preuveneers and Joosen[96] utilized proactivity principle in the design of the solution for a remote health monitoring system. Moreover, the study in the work of Kung et al[97] applied the principle of visibility and transparency to ITSs.

6.2 | Testing and verification

This is a crucial part of the design of a security- and privacy-friendly system to make sure that the implementation of such systems achieves its security and privacy-related requirements. Privacy-related testing and verification should be incorporated into the current testing processes as they are not basically different from other types of testing.[24] The main goal of these verification approaches is to find information leaks from different applications, for instance, by using black box differential testing.[98] The process of testing and verification must be applied in design of any new system architecture in information-centric smart cities.

6.3 | Privacy architecture

Privacy architecture is required to consider various protection approaches to ensure that there are no privacy leakages in the system. For instance, the study in the work of Choi et al[99] proposed an architecture relying on the trustworthy remote data stores and a broker, which intercedes access to the users' data stores. In addition, the study in the work of Layouni et al[100] combined various cryptographic approaches to provide privacy in the system.

6.4 | Data minimization

According to the work of Gürses et al,[101] data minimization should be considered as one the most important parts of the privacy by design strategy. In information-centric smart cities, this strategy can be utilized in various application such as in electronic toll pricing system to analyze different architectural options.[102] It can also be used in the analysis of big data to obtain privacy-protection solutions.[103] In smart cities, smart systems should be designed in a way to avoid recoding unrelated data. For example, cameras for ITSs can also record unrelated information or sensors in smart environments may collect more data rather than needed. Therefore, data minimization techniques can be used to overcome such challenges.

6.5 | Secret sharing

This method allows distribution of secret information among different participants.[24] It is usually divided into m shares with each participant having one share. This method requires at least n shares to recover the secret. Therefore, it provides reliability and confidentiality in the system. In information-centric smart cities, secret sharing can be utilized for distributed data storage,[104] and for data aggregation from smart meters[105] and sensor networks.[106]

6.6 | System security and access control

In information-centric smart cities, security of the system and its subsystems is crucial for the purpose of privacy protection. For example, if there are vulnerabilities in the system, attackers can easily have access to smart devices and retrieve the desired data which would be very dangerous for the privacy of users' sensitive data. Therefore, it is mandatory to secure the system to avoid any attacks from the hackers. Access control restricts the access of data from unauthorized parties. It would also help to minimize control of the system from the misuse of stored data. Access control is also important for autonomous systems with a connection to the internet in which smart devices can be monitored remotely.[107]

6.7 | Secure multiparty computation

It is a cryptographic approach that permits multiple parties to calculate the value of a public function, without showing the private inputs of the parties and without depending on a trusted third party (TTP).[24] In smart cities, this method can be employed in the design of a healthcare system to analyze the results of genomic tests where it is required to keep the test sequence and the patient's genome private.[108]

7 | RECOMMENDED SECURE ARCHITECTURE

An IoT-based smart city architecture operates over heterogeneous networks (HetNets) and consists of millions of resource-constrained devices. In Figure 4, basic components of an IoT-based smart city architecture are shown. These components include black networks (BNs), trusted software-defined networking (SDN) controller named as TTP, unified registry (UR), and key management system (KMS).[109] These four components are responsible for secure communication and authentication across HetNets and have different responsibilities in the architecture. Black networks are responsible for data privacy, integrity, confidentiality and authentication. Trusted third party is responsible for efficient routing across IoT nodes, while UR is used for a database of various devices such as nodes, sensors, and gateways. Finally, KMS is responsible for IoT networks.

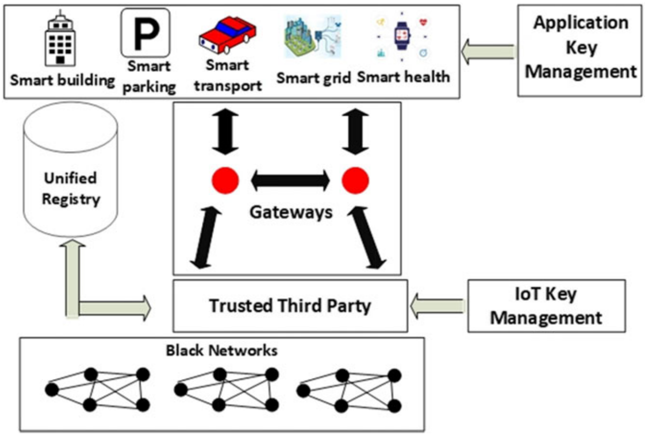

FIGURE 4 An overview of the components of a secure Internet of Things (IoT)–based smart cities architecture

7.1 | Black networks

Black networks are used to secure data that contains the meta-data, related to each packet in an IoT protocol.[110] They can secure data through various encryption methods which can be done viaGrain128a or AES in the EAX or OFB modes. Black networks enable authentication and secure communication at both link layer and network layer.[109] Moreover, BNs can reduce a wide range of active and passive attacks, which, in turn, provides confidentiality, integrity and privacy in IoT-based networks because of the secured communications at the network and the link layer.

7.2 | Trusted SDN controller

Software-defined networking is a paradigm that provides several opportunities to secure the network more efficiently. In this architecture, a SDN controller is used for the communication of network devices using various protocols. OpenFlow is the most commonly used protocol for the communication between various devices in the network and the SDN controller.[111] The main aim of the SDN controller is to resolve the routing challenges in privacy protection of IoT-based BNs.[110] OpenFlow protocol allows the SDN controller to begin a secure connection with the devices in the network. Trusted SDN controller can manage sleep and/or wake cycles, and can keep up a global IoT-based network view.[109]

7.3 | Unified registry

The main purpose of UR is to consolidate the heterogeneous technologies to create IoT-based networks for smart cities. The concept can also be extended to a visiting UR for the IoT nodes that are mobile and cross systems. This is crucial from a security perspective that variety of IoT networks considers fixed nodes communicating through wireless communication technologies. There are several wireless communication technologies utilized in smart cities including W-Fi and Long-Term Evolution. Moreover, many protocols such as IPv6 over low-power wireless personal area networks, ZigBee, and Bluetooth low energy, and several addressing approaches such as IPv6 128-bit addressing, radio frequency identification addressing and Bluetooth 48-bit addressing can be utilized in smart environments. All these technologies, protocols, and schemes require a unified attribute for identity management, authentication and authorization. Furthermore, translation between wireless communication technologies, protocols, and addressing approaches has to be done and UR makes the conversion process easier. It is difficult to implement a UR due to several regulatory, practical, and security issues. However, a logical entity can be implemented in a highly distributed manner that focuses on data and attribute set of an IoT node within the smart cities' network.

7.4 | Key management system

Key management system[109] is the process of managing different tasks associated with various aspects of cryptographic key for cryptosystem. It is an important part of all security infrastructures. In an IoT environment, resource-constrained devices communicate in a secure manner using a symmetric shared key. Keys should be created and stored, and used securely. A critical issue regarding symmetric keys in a distributed mobile system is related to key distribution. Using a hierarchal KMS provides efficient key distribution for symmetric keys in smart cities. It is required to authenticate communications between IoT devices.[112] Moreover, IoT applications require different security protocols and standards as they may deal with different security vulnerabilities. Some of the most commonly used IoT protocols such as message queuing telemetry transport and constrained application protocol do not have built-in security mechanism.[113] However, constrained application protocol and other protocols can utilize protocols such as secure sockets layer to enhance their security. This means that, for secure communication between IoT devices, it is not sufficient to have single factor authentication.[113] Therefore, it is required to have the KMS with two-factor authentication mechanism to mitigate the risk and improve the security in IoT networks.[114]

As an example for such an architecture, consider a node in an IoT BN that wants to send a packet to another node. The SDN controllers can ensure availability and synchronize the nodes for routing by creating the flow tables for the packets to be routed from one node to another. In this regard, UR is responsible for identity management and node authentication and authorization. In addition, KMS provides external key management for the IoT nodes to communicate securely using a shared key.

A summary of the security components and services in IoT-based smart cities is provided in Table 3.

TABLE 3 Components and services of a secure Internet of Things–based architecture for smart cities

Components	Services
BNs	Integrity, confidentiality, privacy
TTP	Availability, secure routing
UR	Identity management, mobility, authentication, authorization
KMS	Efficient key distribution for symmetric keys

Abbreviations: BN, black network; KMS, key management system; TTP, trusted third party; UR, unified registry.

8 | OPEN ISSUES AND FUTURE RESEARCH DIRECTIONS

In spite of different research studies and rapid improvement that have been obtained in recent decade regarding the security and privacy in information-centric smart cities, there are still open research issues and challenges that should be taken into account regarding the improvements of the smart cities in terms of security and privacy.

8.1 | Mobile crowd sensing

Crowd sensing (CS) is a technique where a number of people having mobile devices can extract and share information related to their interests. Crowd sensing sometimes is referred to as mobile CS (MCS) where smart devices such as phones and other wearable devices are emerging as sensing, computing, and communication devices.[115] Mobile CS has a great potential of enhancing people's quality of life in various applications such as healthcare and transportation. Despite all the benefits of MCS, data privacy and user trustworthiness are critical problems, which may be faced by it.[115] Therefore, these challenges are critical for CS in smart cities, which need to be carefully addressed in future research. Moreover, MCS has great environmental and social applications for smart cities. For example, environmental applications of MCS include measuring the level of pollution in a city and the level of water in creeks, and monitoring the natural home of wildlife.[116] Furthermore, in social MCS, users can share their sensed information using a database server, which provides a good understanding of problems related to the community.[116]

8.2 | Big data

The rapid rise in the number of smart devices and big data leads toward the problem of security and privacy in smart cities' applications such as intelligent systems. Attackers can abuse the human intelligence and gain access to the big data to infer and violate the privacy of data owners. There are many techniques such as cryptographic approaches that can be used to detect these attackers. Besides that, it would be beneficial to improve the traceability of the network and allow a TTP to control it. In addition, it is of great importance to achieve data privacy, integrity, authentication, and availability to secure big data.

8.3 | Internet of Things–based network security

The IoT can be considered as HetNets where different networks such as smartphone networks, social networks, internet, and industrial networks are integrated and connected together to provide better services to the people.[117] Due to this complex environment, it is required to conduct research on effective technologies to overcome the latest challenges regarding security and privacy in smart cities. In this regard, development of effective prevention approaches is significantly important. Moreover, it is beneficial to model the spread patterns of data in WSNs.[118]

8.4 | Lightweight security solutions

Several approaches have been developed recently regarding the security and privacy issues in smart cities. However, the application for some of these approaches is not realistic. Due to the availability of resource- and energy-constraint devices (eg, sensors) in smart cities' infrastructures, it is not possible to implement advanced and strong security algorithms. Therefore, it is required to conduct research on developing lightweight security solutions to reduce overhead while providing an acceptable level of protection simultaneously.

8.5 | Authentication and confidentiality

In smart systems, authentication is required to ensure that services in heterogeneous systems can only be accessed by authorized users.[119] The IoT devices in smart cities are capable of authenticating the network itself and other nodes in the network and the messages from the management stations. In addition, since the amount of data authentication is increasing dramatically, it is crucial to develop effective and advanced technologies to ensure exact and real-time authentication in smart cities.

Confidentiality is another requirement for securing smart cities. It prevents information from being subjected to the wrong source or passive attacks. In IoT networks, attackers can access devices and listen secretly to the communication. Therefore, it is important to conduct research into encryption-based techniques to protect confidentiality of data transmission between nodes. This, in turn, helps to have a reliable communication system.[120]

8.6 | Availability and integrity

In smart cities, services should be available whenever they are needed. They should also be capable of maintaining effective actions while they are under attack. Furthermore, a smart system in smart cities should have the ability to discover unusual conditions and must be able to stop more damages to the system. Therefore, it is required to investigate on robust protection techniques to deal with the increasingly smart attacks.

Moreover, integrity of IoT devices and information being exchanged between the devices and the cloud is significantly important. Communications occur between various devices in smart cities; therefore, it is possible to easily damage the data if they are not properly protected during the transmission process. Thus, it is important to investigate on effective methods to guarantee the integrity of data in communication between IoT devices in smart cities.

8.7 | The application of cloud/fog Technology in smart cities

Cloud computing provides a way to locally store and manage an enormous amount of data collected by IoT devices. However, the process of sending such a vast amount of data is costly in terms of storage, bandwidth, latency, and communication. As a result, IBM suggested to process data at the edge of the network using the concept of fog computing, instead of transferring such a huge amount of data to the cloud.[121] Fog computing has several applications in achieving the requirements for building sustainable smart cities such as smart agriculture,[122] smart healthcare,[123] and smart water management.[124] In spite of the important benefits of fog computing for smart cities, several security and privacy challenges need to be taken into account such as data/web security and virtualization.[125] This is due to the limitation of computing resources of fog nodes, which complicates providing security solutions for them.[126] Moreover, the probability of cyberattacks against fog nodes are higher than cloud data centers because they are usually more accessible.

9 | CONCLUSION

Smart cities can improve the functionality of urban environments and enhance the quality of life and the well-being of people. By the implementation of various smart systems, security and privacy challenges have become an important issue which needs efficient and effective solutions. In addition, it is of great importance to consider the security and privacy threats in the design and implementation of new smart systems. In this paper, we have investigated and discussed the security and privacy issues in information-centric smart cities' applications. First, we have introduced some typical applications of smart cities. We then presented the general requirements regarding the security and privacy challenges for smart cities' services. Moreover, we presented a number of security and privacy solutions for various applications of information-centric smart cities. We finally discussed some open research issues that should be carefully taken into account regarding the performance improvement of smart cities in terms of security and privacy.

ORCID

Fadi Al-Turjman https://orcid.org/0000-0001-5418-873X
Hadi Zahmatkesh https://orcid.org/0000-0002-9245-512X

REFERENCES

1. Cui L, Xie G, Qu Y, Gao L, Yang Y. Security and privacy in smart cities: challenges and opportunities. *IEEE Access*. 2018;6:46134-46145.
2. Ever E, Al-Turjman FM, Zahmatkesh H, Riza M. Modelling green HetNets in dynamic ultra-large-scale applications: a case-study for femtocells in smart-cities. *Computer Networks*. 2017;128:78-93.
3. Li Y, Lin Y, Geertman S. The development of smart cities in China. In: Proceedings of the 14th International Conference on Computers in Urban Planning and Urban Management; 2015; Cambridge, MA.

4. Wang M, Wu J, Li G, Li J, Li Q, Wang S. Toward mobility support for information-centric IoV in smart city using fog computing. Paper presented at: IEEE International Conference on Smart Energy Grid Engineering (SEGE); 2017; Oshawa, Canada.
5. Sheng Z, Yang S, Yu Y, Vasilakos AV, McCann JA, Leung KK. A survey on the ietf protocol suite for the Internet of Things: standards, challenges, and opportunities. *IEEE Wirel Commun*. 2013;20(6):91-98.
6. Vasilakos AV, Li Z, Simon G, You W. Information centric network: research challenges and opportunities. *J Netw Comput Appl*. 2015;52:1-10.
7. Mars D, Gammar SM, Lahmadi A, Saidane LA. Using information centric networking in Internet of Things: a survey. *Wirel Pers Commun*. 2019;105:87-103.
8. Lindgren A, Ben Abdesslem F, Ahlgren B, Schelén O, Malik A. Applicability and tradeoffs of information-centric networking for efficient IoT. 2015.
9. Hahm O, Baccelli E, Schmidt TC, Wahlisch M, Adjih C. A named data network approach to energy efficiency in IoT. Paper presented at: 2016 IEEE Globecom Workshops (GC Wkshps); 2016; Washington, DC.
10. Zhang K, Ni J, Yang K, Liang X, Ren J, Shen XS. Security and privacy in smart city applications: challenges and solutions. *IEEE Commun Mag*. 2017;55(1):122-129.
11. Biswas K, Muthukkumarasamy V. Securing smart cities using blockchain technology. Paper presented at: 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS); 2016; Sydney, Australia.
12. Perevezentsev M, Sullivan F. *Strategic Opportunity Analysis of the Global Smart City Market*. Technical report. Frost and Sullivan; 2013.
13. Albino V, Berardi U, Dangelico RM. Smart cities: definitions, dimensions, performance, and initiatives. *J Urban Technol*. 2015;22(1):3-21.
14. *Smart Cities Require Smarter Cybersecurity*. Technical report. 2016. http://www.govtech.com/
15. He Y, Yu FR, Zhao N, Leung VC, Yin H. Software-defined networks with mobile edge computing and caching for smart cities: a big data deep reinforcement learning approach. *IEEE Commun Mag*. 2017;55(12):31-37.
16. Maamar Z, Baker T, Sellami M, Asim M, Ugljanin E, Faci N. Cloud vs edge: who serves the Internet-of-Things better. *Internet Technol Lett*. 2018;1(5):e66.
17. Mahmud R, Kotagiri R, Buyya R. Fog computing: a taxonomy, survey and future directions. In: *Internet of Everything: Algorithms, Methodologies, Technologies and Perspectives*. Singapore: Springer Nature Singapore Pte Ltd; 2018:103-130.
18. Liang K, Zhao L, Chu X, Chen HH. An integrated architecture for software defined and virtualized radio access networks with fog computing. *IEEE Network*. 2017;31(1):80-87.
19. Abbas N, Asim M, Tariq N, Baker T, Abbas S. A mechanism for securing IoT-enabled applications at the fog layer. *J Sens Actuator Netw*. 2019;8(1):16.
20. Cui S, Belguith S, De Alwis P, Asghar MR, Russello G. Collusion defender: preserving subscribers' privacy in publish and subscribe systems. *IEEE Trans Dependable Secure Comput*. 2019:1.
21. Ferraz FS, Sampaio C, Ferraz C. Towards a smart-city security architecture: proposal and analysis of impact of major smart-city security issues. In: Proceedings of the First International Conference on Advances and Trends in Software Engineering (SOFTENG); 2015; Barcelona, Spain.
22. Butt TA, Afzaal MA. Security and privacy in smart cities: issues and current solutions. In: *Smart Technologies and Innovation for a Sustainable Future: Proceedings of the 1st American University in the Emirates International Research Conference - Dubai, UAE 2017*. Cham, Switzerland: Springer Nature Switzerland AG; 2019:317-323.
23. Gharaibeh A, Salahuddin MA, Hussini SJ, et al. Smart cities: a survey on data management, security, and enabling technologies. *IEEE Commun Surv Tutor*. 2017;19(4):2456-2501.
24. Eckhoff D, Wagner I. Privacy in the smart city—applications, technologies, challenges, and solutions. *IEEE Commun Surv Tutor*. 2018;20(1):489-516.
25. Sicari S, Rizzardi A, Grieco LA, Coen-Porisini A. Security, privacy and trust in Internet of Things: the road ahead. *Computer Networks*. 2015;76:146-164.
26. Tan L, Wang N. Future internet: the Internet of Things. Paper presented at: 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE); 2010; Chengdu, China.
27. Hwang I, Shin D. Application level network virtualization using selective connection. Paper presented at: IEEE International Conference on Consumer Electronics (ICCE); 2018; Las Vegas, NV.
28. Anoh K, Ikpehai A, Bajovic D, et al. Virtual microgrids: a management concept for peer-to-peer energy trading. In: Proceedings of the 2nd ACM International Conference on Future Networks and Distributed Systems (ICFNDS); 2018; Amman, Jordan.
29. Gungor VC, Sahin D, Kocak T, et al. Smart grid technologies: communication technologies and standards. *IEEE Trans Ind Inform*. 2011;7(4):529-539.
30. Bello O, Zeadally S. Toward efficient smartification of the Internet of Things (IoT) services. *Futur Gener Comput Syst*. 2019;92:663-673.
31. Aouini I, Azzouz LB. Smart grids cyber security issues and challenges. *Int J Electron Commun Eng*. 2015;9(11):1263-1269.
32. Petinrin JO, Shaaban M. Smart power grid: technologies and applications. Paper presented at: 2012 IEEE International Conference on Power and Energy (PECon); 2012; Kota Kinabalu, Malaysia.
33. Mohanty SP, Choppali U, Kougianos E. Everything you wanted to know about smart cities: the Internet of Things is the backbone. *IEEE Consumer Electron Mag*. 2016;5(3):60-70.
34. Vlahogianni EI, Kepaptsoglou K, Tsetsos V, Karlaftis MG. A real-time parking prediction system for smart cities. *J Intell Transp Syst*. 2016;20(2):192-204.

35. Zanella A, Bui N, Castellani A, Vangelista L, Zorzi M. Internet of Things for smart cities. *IEEE Internet Things J*. 2014;1(1):22-32.
36. Tang B, Chen Z, Hefferman G, Wei T, He H, Yang Q. A hierarchical distributed fog computing architecture for big data analysis in smart cities. In: Proceedings of the ASE Big Data and Social Informatics (ASE BD&SI); 2015; Kaohsiung, Taiwan.
37. Li X, Lu R, Liang X, Shen X, Chen J, Lin X. Smart community: an Internet of Things application. *IEEE Commun Mag*. 2011;49(11):68-75.
38. Ding D, Conti M, Solanas A. A smart health application and its related privacy issues. Paper presented at: Smart City Security and Privacy Workshop (SCSP-W); 2016; Vienna, Austria.
39. Ni J, Lin X, Zhang K, Shen X. Privacy-preserving real-time navigation system using vehicular crowdsourcing. Paper presented at: 2015 IEEE 84th Vehicular Technology Conference (VTC-Fall); 2016; Montreal, Canada.
40. Catarinucci L, de Donno D, Mainetti L, et al. An IoT-aware architecture for smart healthcare systems. *IEEE Internet Things J*. 2015;2(6):515-526.
41. Zhang K, Lu R, Liang X, Qiao J, Shen XS. PARK: a privacy-preserving aggregation scheme with adaptive key management for smart grid. Paper presented at: 2013 IEEE/CIC International Conference on Communications in China (ICCC); 2013; Xi'an, China.
42. Finster S, Baumgart I. Privacy-aware smart metering: a survey. *IEEE Commun Surv Tutor*. 2014;16(3):1732-1745.
43. Gong T, Huang H, Li P, Zhang K, Jiang H. A medical healthcare system for privacy protection based on IoT. Paper presented at: 2015 Seventh IEEE International Symposium on Parallel Architectures, Algorithms and Programming (PAAP); 2015; Nanjing, China.
44. Ning Z, Xia F, Ullah N, Kong X, Hu X. Vehicular social networks: enabling smart mobility. *IEEE Commun Mag*. 2017;55(5):16-55.
45. Wagner M, Kuba M, Oeder A. Smart grid cyber security: a German perspective. Paper presented at: IEEE International Conference on Smart Grid Technology, Economics and Policies (SG-TEP); 2012; Nuremberg, Germany.
46. Delgado-Gomes V, Martins JF, Lima C, Borza PN. Smart grid security issues. Paper presented at: 2015 9th IEEE International Conference on Compatibility and Power Electronics (CPE); 2015; Costa da Caparica, Portugal.
47. Zargar ST, Joshi J, Tipper D. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE Commun Surv Tutor*. 2013;15(4):2046-2069.
48. McGregory S. Preparing for the next DDoS attack. *Network Security*. 2013;2013(5):5-6.
49. Logota E, Mantas G, Rodriguez J, Marques H. Analysis of the impact of denial of service attacks on centralized control in smart cities. In: *Wireless Internet: 8th International Conference, WICON 2014, Lisbon, Portugal, November 13-14, 2014, Revised Selected Papers*. Cham, Switzerland: Institute for Computer Sciences, Social Informatics and Telecommunications Engineering; 2015:91-96.
50. Brewster T. Smart or stupid: will our cities of the future be easier to hack. The Guardian; 2014.
51. AlDairi A, Tawalbeh L. Cyber security attacks on smart cities and associated mobile technologies. *Procedia Comput Sci*. 2017;109:1086-1091.
52. Cédric LB, Darra E, Bachlechner D, et al. *Cyber Security for Smart Cities-an Architecture Model for Public Transport*. ENISA; 2015.
53. Ijaz S, Shah MA, Khan A, Ahmed M. Smart cities: a survey on security concerns. *Int J Adv Comput Sci Appl*. 2016;7(2):612-625.
54. Angrishi K. Turning Internet of Things (IoT) into Internet of Vulnerabilities (IoV): IoT botnets. arXiv preprint arXiv:1702.03681; 2017.
55. Kolias C, Kambourakis G, Stavrou A, Voas J. DDoS in the IoT: Mirai and other botnets. *Computer*. 2017;50(7):80-84.
56. Ghafir I, Prenosil V, Hammoudeh M, et al. BotDet: a system for real time botnet command and control traffic detection. *IEEE Access*. 2018;6:38947-38958.
57. Hutson M. A matter of trust. *Science*. 2017;358(6369):1375-1377.
58. Weber RH. Internet of Things–new security and privacy challenges. *Comput Law Secur Rev*. 2010;26(1):23-30.
59. Elmaghraby AS, Losavio MM. Cyber security challenges in smart cities: safety, security and privacy. *J Adv Res*. 2014;5(4):491-497.
60. Christidis K, Devetsikiotis M. Blockchains and smart contracts for the Internet of Things. *IEEE Access*. 2016;4:2292-2303.
61. Dorri A, Kanhere SS, Jurdak R, Gauravaram P. Blockchain for IoT security and privacy: the case study of a smart home. Paper presented at: 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops); 2017; Kona, HI.
62. Lei A, Cruickshank H, Cao Y, Asuquo P, Ogah CPA, Sun Z. Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. *IEEE Internet Things J*. 2017;4(6):1832-1843.
63. Zyskind G, Nathan O Pentland A. Decentralizing privacy: using blockchain to protect personal data. Paper presented at: 2015 IEEE Security and Privacy Workshops; 2015; San Jose, CA.
64. Fu A, Yu S, Zhang Y, Wang H, Huang C. NPP: a new privacy-aware public auditing scheme for cloud data sharing with group users. *IEEE Trans Big Data*. 2017:1.
65. Neisse R, Steri G, Nai-Fovino I. A blockchain-based approach for data accountability and provenance tracking. In: Proceedings of the 12th ACM International Conference on Availability, Reliability and Security (ARES); 2017; Reggio Calabria, Italy.
66. Laurent M, Kaaniche N, Le C, Vander Plaetse M. A blockchain-based access control scheme. Paper presented at: 15th International Conference on Security and Cryptography (SECRYPT); 2018; Porto, Portugal.
67. Jing Q, Vasilakos AV, Wan J, Lu J, Qiu D. Security of the Internet of Things: perspectives and challenges. *Wireless Networks*. 2014;20(8):2481-2501.
68. Mahmood Z, Ning H, Ghafoor A. Lightweight two-level session key management for end user authentication in Internet of Things. Paper presented at: 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData); 2016; Chengdu, China.
69. Li N, Liu D, Nepal S. Lightweight mutual authentication for IoT and its applications. *IEEE Trans Sustain Comput*. 2017;2(4):359-370.
70. Abdallah A, Shen XS. A lightweight Lattice-based homomorphic privacy-preserving data aggregation scheme for smart grid. *IEEE Trans Smart Grid*. 2018;9(1):396-405.

71. Jabbar I, Najim S. Using fully homomorphic encryption to secure cloud computing. *Internet Things Cloud Comput*. 2016;4(2):13-18.
72. Talpur MSH, Bhuiyan MZA, Wang G. Shared–node IoT network architecture with ubiquitous homomorphic encryption for healthcare monitoring. *Int J Embed Syst*. 2014;7(1):43-54.
73. Alabdulatif A, Khalil I, Forkan ARM, Atiquzzaman M. Real-time secure health surveillance for smarter health communities. *IEEE Commun Mag*. 2019;57(1):122-129.
74. Mackintosh M, Epiphaniou G, Al-Khateeb H, Burnham K, Pillai P, Hammoudeh M. Preliminaries of orthogonal layered defence using functional and assurance controls in industrial control systems. *J Sens Actuator Netw*. 2019;8(1):14.
75. Hao J, Huang C, Ni J, Rong H, Xian M, Shen XS. Fine-grained data access control with attribute-hiding policy for cloud-based IoT. *Computer Networks*. 2019;153:1-10.
76. Cui H, Deng RH, Wu G, Lai J. An efficient and expressive ciphertext-policy attribute-based encryption scheme with partially hidden access structures. In: *Provable Security: 10th International Conference, ProvSec 2016, Nanjing, China, November 10-11, 2016, Proceedings*. Cham, Switzerland: Springer International Publishing AG; 2016:19-38.
77. Zhou L, Su C, Chiu W, Yeh KH. You think, therefore you are: transparent authentication system with brainwave-oriented bio-features for IoT networks. *IEEE Trans Emerg Top Comput*. 2017:1.
78. Amin R, Sherratt RS, Giri D, Islam SH, Khan MK. A software agent enabled biometric security algorithm for secure file access in consumer storage devices. *IEEE Trans Consum Electron*. 2017;63(1):53-61.
79. Natgunanathan I, Mehmood A, Xiang Y, Beliakov G, Yearwood J. Protection of privacy in biometric data. *IEEE Access*. 2016;4:880-892.
80. Wang Y, Wan J, Guo J, Cheung YM, Yuen PC. Inference-based similarity search in randomized Montgomery domains for privacy-preserving biometric identification. *IEEE Trans Pattern Anal Mach Intell*. 2018;40(7):1611-1624.
81. Singandhupe A, La HM, Feil-Seifer D. Reliable security algorithm for drones using individual characteristics from an EEG signal. *IEEE Access*. 2018;6:22976-22986.
82. Alsheikh MA, Lin S, Niyato D, Tan HP. Machine learning in wireless sensor networks: algorithms, strategies, and applications. *IEEE Commun Surv Tutor*. 2014;16(4):1996-2018.
83. Luo X, Zhang D, Yang LT, Liu J, Chang X, Ning H. A kernel machine-based secure data sensing and fusion scheme in wireless sensor networks for the cyber-physical systems. *Futur Gener Comput Syst*. 2016;61:85-96.
84. Aminanto ME, Choi R, Tanuwidjaja HC, Yoo PD, Kim K. Deep abstraction and weighted feature selection for Wi-Fi impersonation detection. *IEEE Trans Inf Forensics Secur*. 2018;13(3):621-636.
85. Shamshirband S, Patel A, Anuar NB, Kiah MLM, Abraham A. Cooperative game theoretic approach using fuzzy Q-learning for detecting and preventing intrusions in wireless sensor networks. *Eng Appl Artif Intel*. 2014;32:228-241.
86. Biggio B, Russu P, Didaci L, Roli F. Adversarial biometric recognition: a review on biometric system security from the adversarial machine-learning perspective. *IEEE Signal Process Mag*. 2015;32(5):31-41.
87. Miller S, Busby-Earle C. The role of machine learning in botnet detection. Paper presented at: 2016 11th IEEE International Conference for Internet Technology and Secured Transactions (ICITST); 2016; Barcelona, Spain.
88. Tsai CW, Lai CF, Chiang MC, Yang LT. Data mining for Internet of Things: a survey. *IEEE Commun Surv Tutor*. 2014;16(1):77-97.
89. Xing K, Hu C, Yu J, Cheng X, Zhang F. Mutual privacy preserving *k*-means clustering in social participatory sensing. *IEEE Trans Ind Inform*. 2017;13(4):2066-2076.
90. Li L, Lu R, Choo KKR, Datta A, Shao J. Privacy-preserving-outsourced association rule mining on vertically partitioned databases. *IEEE Trans Inf Forensics Secur*. 2016;11(8):1847-1861.
91. Saleem J, Hammoudeh M, Raza U, Adebisi B, Ande R. IoT standardisation: challenges, perspectives and solution. In: Proceedings of the 2nd ACM International Conference on Future Networks and Distributed Systems (ICFNDS); 2018; Amman, Jordan.
92. Jerkins JA. Motivating a market or regulatory solution to IoT insecurity with the Mirai botnet code. Paper presented at: 7th IEEE Annual Computing and Communication Workshop and Conference (CCWC); 2017; Las Vegas, NV.
93. Saleem J, Hammoudeh M. Defense methods against social engineering attacks. In: *Computer and Network Security Essentials*. Cham, Switzerland: Springer International Publishing AG; 2018:603-618.
94. Ståhlbröst A, Padyab A, Sällström A, Hollosi D. Design of smart city systems from a privacy perspective. *IADIS Int J WWW/Internet*. 2015;13(1):1-16.
95. Cavoukian A. Privacy by design: the 7 foundational principles. Ontario, Canada: Information and Privacy Commissioner; 2009.
96. Preuveneers D, Joosen W. Privacy-enabled remote health monitoring applications for resource constrained wearable devices. In: Proceedings of the 31st Annual ACM Symposium on Applied Computing (SAC); 2016; Pisa, Italy.
97. Kung A, Freytag JC, Kargl F. Privacy-by-design in ITS applications. Paper presented at: 2011 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks; 2011; Lucca, Italy.
98. Jung J, Sheth A, Greenstein B, Wetherall D, Maganis G, Kohno T, Privacy oracle: a system for finding application leaks with black box differential testing. In: Proceedings of the 15th ACM Conference on Computer and Communications Security (CCS); 2008; Alexandria, VA.
99. Choi H, Chakraborty S, Charbiwala ZM, Srivastava MB. SensorSafe: a framework for privacy-preserving management of personal sensory information. In: *Secure Data Management: 8th VLDB Workshop, SDM 2011, Seattle, WA, USA, September 2, 2011, Proceedings*. Berlin, Germany: Springer-Verlag GmbH Berlin Heidelberg; 2011:85-100.
100. Layouni M, Verslype K, Sandıkkaya MT, De Decker B, Vangheluwe H. Privacy-preserving telemonitoring for ehealth. In: *Data and Applications Security XXIII: 23rd Annual IFIP WG 11.3 Working Conference, Montreal, Canada, July 12-15, 2009. Proceedings*. Berlin, Germany: Springer-Verlag Berlin Heidelberg; 2009:95-110.

101. Gürses S, Troncoso C, Diaz C. Engineering privacy by design. *Comput Priv Data Prot*. 2011;14(3):25.
102. Le Métayer D. Privacy by design: a formal framework for the analysis of architectural choices. In: Proceedings of the Third ACM Conference on Data and Application Security and Privacy (CODASPY); 2013; San Antonio, TX.
103. Monreale A, Rinzivillo S, Pratesi F, Giannotti F, Pedreschi D. Privacy-by-design in big data analytics and social mining. *EPJ Data Science*. 2014;3(1):10.
104. Wang Q, Ren K, Yu S, Lou W. Dependable and secure sensor data storage with dynamic integrity assurance. *ACM Trans Sens Netw*. 2011;8(1). Article No. 9.
105. Kursawe K, Danezis G, Kohlweiss M. Privacy-friendly aggregation for the smart-grid. In: *Privacy Enhancing Technologies: 11th International Symposium, PETS 2011, Waterloo, ON, Canada, July 27-29, 2011. Proceedings*. Berlin, Germany: Springer, Berlin, Heidelberg; 2011:175-191.
106. Shi J, Zhang R, Liu Y, Zhang Y. PriSense: privacy-preserving data aggregation in people-centric urban sensing systems. In: Proceedings IEEE INFOCOM; 2010; San Diego, CA.
107. Denning T, Matuszek C, Koscher K, Smith JR, Kohno T. A spotlight on security and privacy risks with future household robots: attacks and lessons. In: Proceedings of the 11th ACM International Conference on Ubiquitous Computing (UbiComp); 2009; Orlando, FL.
108. Jha S, Kruger L, Shmatikov V. Towards practical privacy for genomic computation. Paper presented at: 2008 IEEE Symposium on Security and Privacy (SP); 2008; Oakland, CA.
109. Chakrabarty S, Engels DW. A secure IoT architecture for smart cities. Paper presented at: 2016 13th IEEE Annual Consumer Communications and Networking Conference (CCNC); 2016; Las Vegas, NV.
110. Chakrabarty S, Engels DW, Thathapudi S. Black SDN for the Internet of Things. Paper presented at: 2015 IEEE 12th International Conference on Mobile Ad Hoc and Sensor Systems; 2015; Dallas, TX.
111. Flauzac O, González C, Hachani A, Nolot F. SDN based architecture for IoT and improvement of the security. Paper presented at: 2015 29th IEEE International Conference on Advanced Information Networking and Applications Workshops; 2015; Gwangju, South Korea.
112. Carlin A, Hammoudeh M, Aldabbas O. Intrusion detection and countermeasure of virtual cloud systems-state of the art and current challenges. *Int J Adv Comput Sci Appl*. 2015;6(6).
113. Kelly D, Hammoudeh M. Optimisation of the public key encryption infrastructure for the Internet of Things. In: Proceedings of the 2nd ACM International Conference on Future Networks and Distributed Systems (ICFNDS); 2018; Amman, Jordan.
114. Shivraj VL, Rajan MA, Singh M, Balamuralidhar P. One time password authentication scheme based on elliptic curves for Internet of Things (IoT). Paper presented at: 2015 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW); 2015; Riyadh, Saudi Arabia.
115. He D, Chan S, Guizani M. User privacy and data trustworthiness in mobile crowd sensing. *IEEE Wirel Commun*. 2015;22(1):28-34.
116. Song H, Srinivasan R, Sookoor T, Jeschke S. *Smart Cities: Foundations, Principles, and Applications*. Hoboken, NJ: John Wiley and Sons; 2017.
117. Xu K, Qu Y, Yang K. A tutorial on the Internet of Things: from a heterogeneous network integration perspective. *IEEE Network*. 2016;30(2):102-108.
118. Yu S, Gu G, Barnawi A, Guo S, Stojmenovic I. Malware propagation in large-scale networks. *IEEE Trans Knowl Data Eng*. 2015;27(1):170-179.
119. He D, Zeadally S, Kumar N, Lee JH. Anonymous authentication for wireless body area networks with provable security. *IEEE Syst J*. 2017;11(4):2590-2601.
120. Angelakis V, Tragos E, Pöhls H, Kapovits A, Bassi A. *Designing, Developing, and Facilitating Smart Cities: Urban Design to IoT Solutions*. Cham, Switzerland: Springer International Publishing Switzerland; 2017.
121. Sookhak M, Yu FR, He Y, et al. Fog vehicular computing: augmentation of fog computing using vehicular cloud computing. *IEEE Veh Technol Mag*. 2017;12(3):55-64.
122. Commonwealth Scientific and Industrial Research Organisation (CSIRO). *Phenonet: Distributed Sensor Network for Phenomics Supported by High Resolution Plant Phenomics Centre, CSIRO ICT Centre, and CSIRO Sensor and Sensor Networks TCP*. Technical report. 2011.
123. Zao JK, Gan TT, You CK, et al. Augmented brain computer interaction based on fog computing and linked data. Paper presented at: 2014 International Conference on Intelligent Environments; 2014; Shanghai, China.
124. Perera C, Qin Y, Estrella JC, Reiff-Marganiec S, Vasilakos AV. Fog computing for sustainable smart cities: a survey. *ACM Comput Surv*. 2017;50(3). Article No. 32.
125. Sookhak M, Yu R, Zomaya A. Auditing big data storage in cloud computing using divide and conquer tables. *IEEE Trans Parallel Distributed Syst*. 2018;29(5):999-1012.
126. Zhang P, Liu JK, Yu FR, Sookhak M, Au MH, Luo X. A survey on access control in fog computing. *IEEE Commun Mag*. 2018;56(2):144-149.

How to cite this article: Al-Turjman F, Zahmatkesh H, Shahroze R. An overview of security and privacy in smart cities' IoT communications. *Trans Emerging Tel Tech*. 2019;e3677. https://doi.org/10.1002/ett.3677