Security and Privacy in Smart Cities: Challenges and Opportunities

Saleem Ahmed

Graduate School, IIC University of Technology

Abstract

Internet of Things (IoT) model is action it possible for everyday objects to combine with the Internet. This has put the foundations for the starting of future Smart cities based on systems that consist of a raise of IoT devices to enable story applications. The smart cities model deals with the public data that is recumbent to different security and privacy risks at different level of smart cities architecture. Therefore, the importance of ensuring security and privacy is fundamental in this model. This paper focuses on the security and privacy issues involved in the smart cities. The paper highlights the key applications of smart cities and then check its architecture from security point of view. The paper also reviews the current security and privacy solutions for smart cities and confirm the open issues and research challenges that still need to be declaim in this new model, Internet of Things (IoT) model is making it possible for everyday objects to integrate with the Internet. This has laid the establishment for the inception of future Smart cities based on systems that consist of a raise of IoT devices to enable novel applications. The smart cities model deals with the public data that is prone to different security and privacy risks at different level of smart cities architecture. Therefore, the importance of ensuring security and privacy is essential in this model. This paper focuses on the safety and privacy issues implicated in the smart cities. The paper highlights the key applications of smart cities and then investigates its architecture from security point of view. The paper also reviews the current security and privacy solutions for smart cities and emphasizes the open issues and research challenges that still need to be addressed in this new model.

Keywords

Security, privacy, smart cities, challenge, opportunity.

I. INTRODUCTION

The progress of Information Technology (IT) is impacting human life in multifaceted ways. Information and Communication Technology (ICT) resources are heavily deployed and enhancing the provision of services in our daily lives. The excessive use of ICT resources can be measured from the fact that door locks, window curtains, curtains, TVs, cars, toasters, air conditioners, coffee machines etc. can be controlled through smart phones. In the current era, the concepts like smart commerce, smart environment, smart communication, and smart mobility have emerged to take the impact of ICT to the next level in the form of smart cities[1].

Smart cities involve a large number of sensors collecting and sending data to base station, and other Internet enabled devices which communicate with each other in order to process data. Each of these millions of devices continuously generates important data which are transmitted through heterogeneous networks to appropriate data centers for processing. After processing, certain decisions are taken based upon the analytics [2].

Data is the most important asset for any individual in the smart world. This data may include location coordinates, travelling history, credit card numbers, and medical records to name a few. These data are handled by pieces of hardware and software which might have some vulnerabilities, which can be exploited to get unauthorized access to the data [3].

False data can be injected in good one in order to mislead the decisions taken by concerned parties. Forged health care data may lead to the wrong prescription of medicine, which eventually may result in severe health consequences for the patient.

GPS enabled smart phones may pose a severe threat to owners' privacy. Usually we set the GPS coordinates o four home and office as the originating point. Also, latests mart phones store the route taken by the smart phone carrier which can be used to track their whereabouts. Access to these GPS data can disclose the absence from a certain point which may eventually attract the burglars and intruders [4].

This paper takes an Architectural point of view to determine the Security and privacy issues in the smart cities. Further more, this paper identifies the current security solutions and research challenges in enabling security and privacy in smart city. Sections 2 and 3 cover the details of smart city's architecture and applications, and the security and privacy vulnerabilities are highlighted in Sect. 4.

Finally, Sect. 5 covers the current security solutions and research challenges and then paper is concluded.

II. Smart City Architecture

Smart city intelligent applications rely on data harvested by ubiquitous sensors. These data is transmitted to the cloud by the integration layer that manages the heterogeneity of sensor devices and networks. The architecture of a smart city is thus composed of Perception, Integration, Cloud, Application and business layers as shown in Fig.1.Further more,the security and management is require data lllayers.

A. PerceptionLayer

This layer perceives the environment and in response generates the data. The devices involve at this layer ranges from the RFID tag to smartphones[5].The main goal of this layer is to sense the environment and identify objects/things to collect data.

B. IntegrationLayer

Integration layer is fed with the data collected by the perception layer. The purpose of this layer is to integrate the heterogeneous networks to the cloud layer. Therefore, its role is akin to the network layer in TCP/IP protocol suite. There is a vast diversity of the communication protocols employed by the sensor devices depending on the capabilities of the devices. The communication protocols include RFID, Zigbee,6LowPAN, Bluetooth, Wi-Fi, 4G etc. [6]. Therefore, there are a range of systems that required to be integrated into the overall smart city architecture. This layer fulfills these integration requirements by passing the received data to Cloud layer.

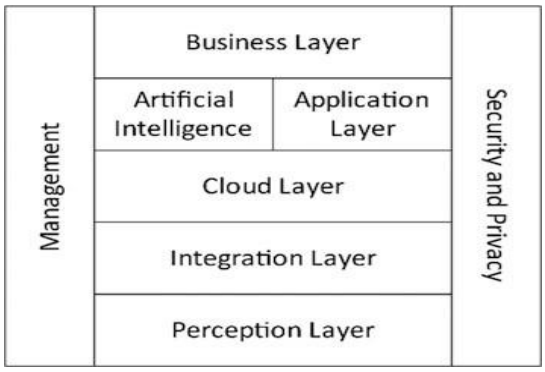

Fig. 1 Smart city's architecture

C. CloudLayer

Cloud layer is the major layer that includes many components such as storage, computation and analytics [7]. This layer receives data from the Integration layer to process and store it for the consumption of Smart cities applications. At this layer, all the things in a smart city are represented by virtual things. These virtual things will make the availability possible for those real physical things that need to sleep most of the time to save their energy consumption. The huge sets of data received at this layer is stored and managed by Big Data technologies[8].

D. ApplicationLayer

As name suggests, different smart city's applications operate at this layer. Some applications also perform analytics to the collected data to aid different smart cities applications. Furthermore, the smart autonomous applications based on Artificial Intelligence execute at this layer[9].

E. BusinessLayer

Business layer helps to create different business model based on services provided by the smart city system. Different services are created using the processed data and those services are further composed into new services to offer new value-added services to the users of as mart city.

III. Smart City Applications

Smart city paradigm opens new avenue for novel applications by connecting the physical world with the ICT systems. The data harvested from these physical spaces are processed and made available in the form of different services that allow applications to use the sensed data or control the physical world, as shown in Fig. 2. This section covers the detail of few key categories of applications in a smart city.

A. Smart Transportation

The smart transportation concept is the materialization of Intelligent Transport System(ITS).This application uses the smart city's processed data to manage the mobility demands of a city such as congestion management, real-time predictions of local transport arrivals, parking space management, and real-time freeway management etc.[10].

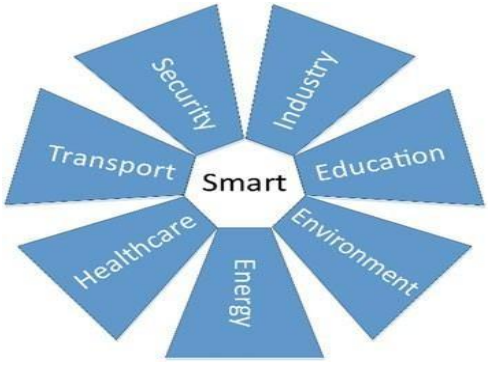

Fig. 2 Smart city application categories

B. Smart Energy

Reducing the energy consumption and to prevent the failure of a power grid for a city or an individual consumer are a few of the many challenges for a city management authority[11].Smart energy applications utilize the widely deployed sensor data to monitor and manage energy from its generation to its consumption. The applications allow authorities to make all individuals accountable to their energy usage and carbon footprint.

C. Smart Healthcare

Smart healthcare applications aim to improve quality of current healthcare systems by continuously monitoring patients' real-time data to diagnose infectious diseases at early stages [12]. Furthermore, it provides the functionality of medical surveillance for people suffering with chronic diseases and remote consultation. The applications consume the cloud services that provides the processed health data, such as ECG and EIT signals that gathered from wearable and other sensor devices. The big data element enables smart healthcare applications to track down the trends to avoid spread of infections and plagues.

D. Smart Education

Smart Education applications exploit the data gathered from different sources in the field to enable active learning in a smart city [13]. The data are collected from infrastructure, people and information that is processed by big data technologies. The process of education is improved by the pro- vision of smart services. Furthermore, this knowledge based society is being further extended to remote areas to improve the life of the people.

E. Smart Environment

This category of applications deals in making different environments, smart by controlling vastly deployed sensor devices [14]. These applications intelligently manage cli- mate with the aid of ubiquitous sensing and actuation. Few examples of these applications include building management, city noise management, CO_2 heavy area detection and management, green reserve management, and resource waste control systems.

F. Smart Security

These applications rely on the sensors based context-aware security systems to provider is k prevention applications[15]. These applications provide the ever needed a security solution to ensure public safety against extreme natural disasters and terrorists.

G. Smart Industry

Smart Industry based applications are committed to support Industry 4.0 era [16]. These applications provide a basis for autonomous intelligent machines that will use the data generated by heterogeneous sensor devices. This reduces the downtime of machines and real-time data flow to assist supply chain management. Overall, these applications will benefit the industry by improving the working conditions while saving on the cost involved in labor and energy.

IV. Security and Privacy Issues

Smart cities can't be considered smart unless these can provide the required level of security. The general security and privacy requirements include ensuring availability, integrity, privacy, access control, confidentiality, and non- repudiation. The smart city harnesses sensed data from physical spaces that contains granular details about the people living in those environments. The journey of this data starts at a sensor node and ends at the user application. Therefore, the smart city poses unique security requirements because it's a system of interlinked systems that share data with each other. This the key argument that discourages the wide-spread usage of smart city services.

The architecture of a smart city can be described as a complex integration of different systems to provide various city-wide services, as shown in Fig. 1.

However, any device running a software is posed to different vulnerabilities, this list of vulner abilities increased rapidly when the device joins a network, because no wit can be remotely hacked as well the smart city consists of millions of devices, therefore, even one single device will make the whole collection vulnerable. The hackers can perform range

of cyber-attacks by exploiting the vulnerabilities.

A. Types of Security and Privacy

The security requirements of as mart city can be divided into two categories. The operational security requirement is to ensure that the employed technology and infrastructure is secure and is immune to any cyber-attack. The second is related to the data that is generated and communicated within the infrastructure using different technologies. How-ever, the data security and protection is dependent on the operational security, as anyone who will break into a system will be capable to violate the data access policy.

Privacy. Privacy, the state of being isolated from undesired attention and heed, is a basic human right as described in many declarations and jurisdictions [17]. However, the concept of privacy differs according to different cultures, contexts and the type of information. Privacy has various dimensions:

- Identity privacy deals with the protection of personal data related to an individual.
- Bodily privacy focus on the protection of physical aspects.
- Territorial privacy protects the personal property and space of an individual.
- Mobility privacy aims to secure the location coordinates and protection against tracking.
- Communications privacy deals with the protection of the communication channels against eavesdropping. These channels include, but not limited to hardware devices which facilitate the data transfer, communication mediums either wired or wireless.
- Transactions privacy focuses to protect the queries and responses against monitoring.

Categories of Attacks. The cyber-attacks are generally categorized into one of these three attacks:

1. Availability attacks: This classification is for attacks that either deny some services or completely bring the system down.
2. Confidentiality attacks: These attacks are related to the unauthorized monitoring and information access.
3. Integrity attacks: These attacks seek to break into system to amalgamate or alter the stored information. Further- more, these attacks alter the configurations such as stopping critical services, infecting system with viruses or making the system inefficient.

B. Security Vulnerabilities and Issues in Smart Cities

A system's security vulnerability explains the security hole that can be caused by number of issues such as weak encryption, human error etc. In a smart city this issue is further aggravated by physically dispersed sensors in public spaces and the system's multifold complexity and interdependencies between its components that makes it vulnerable to various cyber-attacks.

Constrained Devices at Perception Layer. Internet of Things connects all RFID and sensor devices to the Internet. RFID based objects are passive as they require a reader and a gateway to connect to the Internet e.g. smart cards used for transport systems. On the other hand, sensor devices include sensors, actuators and microcontrollers. Now a days, there are variety of sensors available to sense diverse phenomenon such as temperature humidity, location, velocity, proximity, etc. Moreover, the traditionally dumb devices e.g. electronic devices, doors and even lights are notifying and being remotely controlled by users. Most of these sensor devices are constrained in resources and have no effective security or privacy mechanism [18]. This makes these devices prone to be hacked and open sportal for all sort of security risks.

Weak Encryption. One of the traditional way to secure a networked software device is to utilize encryption. It is believed that the encrypted channel ensures the system protection against attackers. The current smart city initiatives are deploying systems without testing them for cyber-security threats. However, it is an important as pectin as mart cities where majority of the IoT devices have constraints and can't support viable encrypted links. Even the encrypted links are prone to other security issues because attackers can still break into encrypted systems using side-channel and cold boot attacks. These issues are the main hurdle in the way of wide acceptance of smart city systems. Communication Technologies at Integration Layer.

There are various communication technologies that are used by different IoT devices depending on their capabilities. These technologies include RFID, NFC,Bluetooth,BLE,ZigBee,6LoWPANbasedonIEE E802.15.4,Wi-Fi,LPWAN(LowPowerWide-area-network),3G and 4G mobile technologies. All these technologies have security vulner abilities that make these susceptible to be hijacked[19]. Even the most sophisticated technologies such as 4Gmobile technologies have vulner abilities in its infrastructure. Cloud Layer. The cloud layer provides the required flexibility to supports calability in smart cities. However, cloud systems also have security issues such as Outs ourcing, Multi-tenancy and massive data that requires intense computation. Outsourcing requires to provide remote access that results in less control on data and eventually causes insecurity and privacy violations. This can be dealt with by making sure that cloud provider is trustworthy and the out- sourced data is verifiable from security and privacy perspectives. Multi-tenancy enables multiple users to utilize the cloud platform. The cloud can use different resource allocation policies to store data of different users on a

single physical machine. Therefore, multi-tenancy poses several security vulnerabilities [20]. Another aspect related to cloud computing is that traditional security techniques requires heavy communication or computation overhead to deal with cloud's massive amount of data. This overhead becomes infeasible e.g. in case of hashing the entire data set that is remotely stored. System's Complexity and Cascade Effect. Smart city systems are large-scale and complex systems containing heterogeneous devices and networks. The smart city's architecture (Fig. 1) has multiple layers where each layer is composed of plethora of devices and technologies. The web of interdependencies between its components and with other systems pose a big challenge to measure and mitigate riskin presence of many stakeholders. The multiple links between system components expose them to security risks even each system is independently secured. Moreover, these interdependencies become an issue while maintaining or upgrading an interface of a system component. The highly interconnected components are also prone to create cascade effects, where an attack on one system e.g. Smart Transport can severely affects other systems as well. This security risk greatly challenges the realization of a smart city where one successful attack can bring down all systems of a city management.

Software Bugs. A software based device can be come vulnerable to cyber-attacks because of software bugs, which leave holes for attackers to sneak into a system. This factor is further intensifies incomplex systems that contain millions of lines of codes where these bugs can open a backdoor for attackers. Once an attacker enters as mart city system then he can get the control of the system and exploit the available data.

User Equipment. Different users of a Smart city are able to consume value-added services and participate in crowd- sensing [4] by using their mobile devices that are prone to many vulnerabilities. Firstly, each mobile phone can be uniquely identified by its IMEI(International Mobile Station Equipment Identity). This IMEI can be related to an owner to get his personal information and can be used to track a mobile device. Furthermore, many users have reckless behavior towards giving access permissions to malicious applications. Once such application will get a permission it can access user's information and control the device.

Human Factor. The smart city systems are hardly allowed to operate fully autonomously, because these systems can cause Kafkaesque situations. Therefore, the human are almost always are in the loop of decision making with some of interaction with the smart city systems [21]. The human error either by mistake or deliberate can result in data leakage or system malfunction. There are many ways in which a smart city user with authority e.g. the municipality's employee can sabotage the system.

Legacy Systems. Legacy systems are everywhere and most of the authorities require to integrate the existing infrastructure to a smart city. Most of the legacy systems are insecure and mostly created decades ago without taking into account the today's security challenges. These systems are not regularly upgraded and have inherent vulnerabilities, thus provide a freeway to attackers. Even new systems in a smart city require to be regularly patched ideally without any downtime.

C. Stakeholders in a Smart City DPIA

In order to perform a DPIA, some preliminary issues should be tackled. The first one is to understand and describe the target of evaluation of the DPIA. This activity should be carried out by the city's DPO in cooperation with the DPOC and DPC. The DPO should define the objects, services or processes which may need to be assessed, and the DPOC should validate it. The target of evaluation (ToE) specifies the scope of the evaluation from a data protection standpoint. It may include one or several components of a smart city, like an app, a system of sensors, cameras, an interface, a database, etc. The same applies to smart cities' services, such as a service offered to citizens in the context of an efficient traffic management. As the WP29 points out in the Guidelines on Data Protection Impact Assessment (hereinafter "DPIA Guidelines"), "a single DPIA could be used to assess multiple processing operations that are similar in terms of the risks presented, provided adequate consideration is given to the specific nature, scope, context and purposes of the processing". For example, a group of municipal authorities setting up a similar network of sensors used to monitor the noise on the streets could carry out a single DPIA covering the processing by these separate controllers. An accurate specification of the ToE is of fundamental importance for the performance of a DPIA, as it is the object thereof. At the beginning of the DPIA report, the person in charge of the DPIA shall accurately determine the ToE and its area of application. This requires to identify, clarify and analyse the data flows. It will usually require to have at least one or several drawings to visualise and analyse all the data flows. On that basis, the legal provisions applicable for the processing of personal data will be determined.[3]The following relevant questions should be answered for each envisaged ToE:

- Does the ToE qualify as an IT product, an IT-based service or processing operation?
- If the ToE is an IT-based product: Does the product manufacturer qualify as a controller ("controller") or as a processor ("processor") in terms of EU data protection law?
- If the ToE is an IT-based service: Does the service provider qualify as a controller

("controller") or as a processor ("processor") in terms of EU data protection law?
- If the ToE is a set of processing operations: Do these operations present similar risks? Can they be covered by the same DPIA?
- What precisely is the target of evaluation?
- What types of personal data are processed when the product or service is used or when the processing operations take place?
- Which groups of data subjects are concerned when the product or service is used (e.g. consumers, citizens, travellers, drivers and employees of the service provider)?
- What data flows occur when the product or service is used? The DPIA must be led by the respective DPO of each city. The DPO shall have an adequate understanding of the GDPR and data protection law. Any DPIA process must encompass at least the following four elements.

D. Privacy App

It is unlikely to easily get a prior informed consent of citizens to get personal data collected in an urban environment. As a consequence, the lawfulness of personal data collection in smart cities usually relies on the public interest and a legal basis. Despite the ability of smart cities to avoid the prior informed consent process, Article 12 of the GDPR requires that data controllers "*take appropriate measures to provide any information (...) relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form*".

Smart cities are particularly complex environments for GDPR implementation, where multiple stakeholders interact and can deploy IoT solutions. Information such as the purpose for data collection and the identity of the data controllers are not easily identifiable. Moreover, the inherent large-scale nature of IoT deployment and public space monitoring is a source of additional risks and obligations.

Beyond the difficulty in acquiring prior informed consent from data subjects in the context of IoT deployments, there are additional key obligations that a data controller should respect. Among those obligations, it is essential to mention not only the obligation to inform data subjects about any personal data processing but also the obligation for the data controllers to ease the exercise of data subject rights.

In this context, Synchrony City designed and developed a dedicated smart phone application to support GDPR implementation and compliance in the context of smart cities. This application has been named Privacy App[4] and is freely available for both Android and iPhone smart phones in several languages.

The application enables smart cities to share information on all deployed IoT devices. The information is accessible through an interactive map that displays the location of each deployed IoT device. It enables smart cities to inform citizens on each and every IoT device deployed in their city. By simply clicking on one of the IoT icons on the map, citizens access to detailed information, including on the purpose of data collection, the data retention period, the data controller, who can access the data, etc. It also enables data subjects to directly contact the data protection officer of the corresponding data controller.

In parallel, the developed application enables citizens to identify any IoT devices that are not yet listed on the map. The citizen can take a picture and tag any IoT device. A moderator, in principle linked to the municipality, is then invited to complement the information.

Such bidirectional model contributes to empowering and engaging with citizens for the collective control of IoT deployments in public space. Furthermore, it enables municipalities to benefit from a crowd sourcing mechanism to identify any illicit IoT deployment in the public space.

V. Security and Privacy Solutions

RFID tags are extensively used in smart city applications. This RFID proliferation has given rise to many security concerns like eavesdropping and threats to privacy of tag owner. Many solutions have been proposed to deal with these issues. An RFID tag identification algorithm [22] ensures secure identification of multiple RFID tags simultaneously and RFID reader authentication with low computational power. SASI [23], another RFID authentication protocol, is a more robust and ultra-lightweight scheme which provides strong authentication and integrity for the communication between RFID tags and its reader. Both these schemes needless computational power for encryption purposes which is why they are preferred.

In order to keep smart city sensor devices secure from intruders, they should be placed in a location where access is restricted and they are out of reach of unauthorized personnel. Whenever a smart city sensor is deployed in the network, it should be authenticated to check if it is authorized to collect and send data in that network. An authentication scheme [24] facilitates key establishment and ensures that only authorized devices with proper credentials can participate in communication with an access point. A com- pressed version of IP Sec [25] can be used for end-to-end encrypted communication

between a smart city sensor device and an IPv6 enable device to ensure privacy.

Integration layer gets data from sensors and delivers to the cloud layer. For this purpose, it uses different communication protocols like Zigbee,6LoWPAN, Bluetooth, Wi-Fi etc. Anyone in the coverage area of these communication technologies can grab the packets resulting income promise of data privacy. This issue can be overcome by encrypting the packets using strong encryption techniques. The constraints of lower computation power and limited memory inside smart city sensors lead us to use lightweight cryptographic algorithms[25].

The exposure of data processed and stored on cloud servers is another issue. Holomorphic encryption algorithms provide the ease of processing encrypted data coming from different sources [26, 27]. This way the privacy of data is ensured without halting the processing pipeline while getting the same results.

The smart city devices use different software to perform their actions. The bugs in the software provide the backdoor to potential adversaries to exploit the functionality and integrity of smart city applications. These weaknesses in software can be avoided by training the developers about writing secure code and embedding security concepts in the software at each stage in Software Development Life Cycle [28–30]. Moreover, the software should be passed through different testing phases to discover any security holes and potential vulnerabilities.

VI. Future Research Challenges

Limited computational power in smart city sensor devices makes them unsuitable for high level computations done with cryptography. Moreover, constrained memory in them also make them in appropriate for large key sizes for encryption/ decryption.

Due to its requirement for high computational power, Public Key Infrastructure (PKI) cannot be used on devices like smart city sensors. An edge-router based authentication scheme uses PKI over IPv6 [31], but it increases the over- head and limits the scalability. Therefore, more research is required to find some alternative of PKI, which requires low computational power and hence consumed less energy.

Smart city sensors are integrated with the system to work uniformly. This integration is made possible in terms of the interdependencies among them. If one component is com-promised ,it may open doors for hackers to the other devices as well. This may have a cascading effect upon the smart city components and result in the failure of the whole system. This opens new research directions to mitigate the inter dependencies and to bind the adversarial effects only to the compromised system.

Users participating in crowd sensing may give access to malicious parties to their personal data. This grant of access might be unintentional because of lack of awareness and use of apps which may affect the system's security. There is a need to spread awareness about the secure use of mobile devices and a strict control over the release of apps.

Legacy systems have been in use for a long time and it is not easy to replace them at once. These systems were designed without considering the security challenges we are facing today. Many vulnerabilities have been already dis- covered and their patches are also available. The problem is that the system owners do not apply the patches regularly. Also the patches are usually designed by inexperienced programmer and they may introduce new vulnerabilities

VII. Conclusion

Smart cities are complex systems that are composed of heterogeneous devices that communicate using a plethora of protocols. These devices and protocols are vulnerable to many security and privacy issues. This paper describes the smart city's architecture and applications. Furthermore, it reviews the security and privacy issues in a smart city from the perspective of its architecture. It also discusses the available solutions pertinent to these issues and highlights the open research challenges in the realization of a secure smart city. RFID tags are extensively used in smart city applications. This RFID proliferation has given rise to many security concerns like eavesdropping and threats to privacy of tag owner. Many solutions have been proposed to deal with these issues. An RFID tag identification algorithm [22] ensures secure identification of multiple RFID tags simultaneously and RFID reader authentication with low computational power. SASI [23], another RFID authentication protocol, is a more robust and ultra-lightweight scheme which provides strong authentication and integrity for the communication between RFID tags and its reader. Both these schemes needless computational power for encryption purposes which is why they are preferred.

References

[1] Hernández Muñoz,J.M.,Vercher,J.B.,Muñoz,L.,Galache,J.A., Presser, M., Gómez, L.A.H., Pettersson, J.: Smart Cities at the Fore front of the Future Internet,pp.447–462(2011)

[2] Albino,V.,Berardi,U.,Dangelico,R.M.:SmartCities:definition s, Dimensions, Performance, and Initiatives, vol. 22, pp. 3–21. Taylor & Francis(2015)

[3] Popescul, D., Radu, L.D.: Data Security in Smart Cities: challenges and Solutions, vol. 20, p. 29. Inforce Association (2016)

[4] Yang, K., Zhang, K., Ren, J., Shen, X.: Security and Privacy in Mobile Crowdsourcing Networks: challenges and Opportunities, vol. 53, pp. 75–81. IEEE(2015)

[5] Zanella, A., Bui, N., Castellani, A., Vangelista, L., Zorzi, M.: InternetofThingsforSmartCities,vol.1,pp.22–32.IEEE(2014)

[6] Yaqoob, I., Hashem, I.A.T., Mehmood, Y., Gani, A., Mokhtar, S., Guizani, S.: Enabling Communication Technologies for Smart Cities,vol.55,pp.112–120.IEEE(2017)
[7] Petrolo,R.,Loscri,V.,Mitton,N.:Towardsa Smart City Basedon Cloud of Things, a Survey on the Smart City Vision and Paradigms,vol.28.WileyOnlineLibrary(2017)
[8] Hashem,I.A.T.,Chang,V.,Anuar,N.B.,Adewole,K.,Yaqoob,I. , Gani, A., Ahmed, E., Chiroma, H.: The Role of Big Data in Smart City,vol.36,pp.748–758.Elsevier(2016)
[9] Al Nuaimi, E., Al Neyadi, H., Mohamed, N., Al-Jaroodi, J.: Applications of Big Data to Smart Cities, vol. 6, p. 25. Springer (2015)
[10] Xiong, Z., Sheng, H., Rong, W., Cooper, D.E.: Intelligent transportation systems for smart cities: a progress review. Sci. China Inf. Sci., 1–7(2012)
[11] Karnouskos, S., Da Silva, P.G., Ilic, D.: Energy Services for the Smart Grid City, pp. 1–6(2012)
[12] Solanas, A., Patsakis, C., Conti, M., Vlachos, I.S., Ramos, V., Falcone, F., Postolache, O., Pérez-Martínez, P.A., Di Pietro, R., Perrea, D.N., et al. Smart Health: a Context-Aware Health ParadigmWithinSmartCities,vol.52,pp.74–81.IEEE(2014)
[13] Jeong, J.-S., Kim, M., Yoo, K.-H.: A Content Oriented Smart Education System Basedon Cloud Computing. Citeseer(2013
[14] Filipponi,L.,Vitaletti,A.,Landi,G.,Memeo,V.,Laura,G.,Puc ci, P.: Smart City: an Event Driven Architecture for Monitoring Public Spaces with Heterogeneous Sensors, pp. 281–286(2010)
[15] Al-Muhtadi, J., Ranganathan, A., Campbell, R., Mickunas, M.D.:Cerberus: a Context-Aware Security Scheme for Smart Spaces,pp. 489–496(2003)
[16] Lee, J., Kao, H.-A., Yang, S.: Service Innovation and Smart Analytics for Industry 4.0 and Big Data Environment, vol. 16, pp. 3–8. Elsevier(2014)
[17] Martínez-Ballesté, A., Pérez-Martínez, P.A., Solanas, A.: The Pursuit of Citizens' Privacy: a Privacy-Aware Smart City is Possible,vol.51,pp.136–141.IEEE(2013)
[18] Granjal, J., Monteiro, E., Silva, J.S.: Security for the internet of things:a survey of existing protocols and open research issues, vol. 17, pp. 1294–1312. IEEE(2015)
[19] Jing, Q., Vasilakos, A.V., Wan, J., Lu, J., Qiu, D.: Security of the Internet of Things: perspectives and Challenges, vol.20,pp.2481– 2501. Springer(2014)
[20] Xiao, Z., Xiao, Y.: Security and Privacy in Cloud Computing,vol.15, pp. 843–859. IEEE(2013).
[21] Nam, T., Pardo, T.A.: Conceptualizing Smart City with Dimen-sions of Technology, People, and Institutions, pp. 282–291(2011)
[22] Karthikeyan, S., Nesterenko, M.: RFID Security Without Exten- sive Cryptography, pp. 63–67(2005)
[23] Chien, H.-Y.: SASI: a New Ultra lightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity, vol. 4, pp. 337–340. IEEE(2007)
[24] Qiu, Y., Ma, M.: An authentication and key establishment scheme to enhance security for M2M in 6LoWPANs. In: 2015 IEEE International Conference on Communication Workshop (ICCW) (2015)
[25] Engels,D.W.,Saarinen,M.J.O.,Schweitzer,P.,Smith,E.M.: The Humming bird-2 Lightweight Authenticated Encryption Algorithm, vol. 11, pp. 19–31.Springer(2011)
[26] Tebaa, M., El Hajji, S., El Ghazi, A.: Homomorphic Encryption Appl.CloudComput.Secur.1,4–6(2012)
[27] López-Alt, A., Tromer, E., Vaikuntanathan, V.: On-the-fly Mul- tiparty Computation on the Cloud via Multikey Fully Homomor- phic Encryption, pp. 1219–1234(2012)
[28] Brown, M., Paller, A.: Secure software development: why the development world awoke to the challenge. Inf. Secur. Techn. Rep. 13(1), 40–43(2008)
[29] Kang, J., Park, J.H.: A secure-coding and vulnerability check system based on smart-fuzzing and exploit. Neurocomputing (2017)
[30] Khan,R.:Secure software development:a prescriptive framework. Comput. Fraud Secur. 2011(8), 12–20(2011)
[31] Goswami, S., Misra, S., Taneja, C., Mukherjee, A.: Securing intra-communication in 6LoWPAN: a PKI integrated scheme. In: 2014 IEEE International Conference on Advanced Networks and Tele communcations Systems (ANTS)(2014)