Building Secure Urban Information Systems Based on IoT Technologies

Oleksii Duda[1[0000-0003-2007-1271]], Nataliia Kunanets[2[0000-0003-3007-2462]], Serhii Martsenko[1[0000-0003-2205-0204]], Oleksandr Matsiuk[1[0000-0003-0204-3971]] and Volodymyr Pasichnyk[2[0000-0002-5231-6395]]

[1] Ternopil Ivan Puluj National Technical University, Ternopil, Ukraine,
[2] Lviv Polytechnic National University, Lviv, Ukraine
oleksij.duda@gmail.com, marcenko@cei.net.ua,
oleksandr.matsiuk@gmail.com
nek.lviv@gmail.com, vpasichnyk@gmail.com

Abstract. An analysis of the state-of-the-art research on methods and tools for building secure urban information systems based on IoT technology reveals the increased interest of a wide range of researchers, the wide range of methods and means they offer to increase the level of security in such systems, and the high fragmentation and fragility of the proposed solutions. Analyzing and improving approaches to addressing security issues when building urban information systems based on IoT devices should be undertaken in the context of all levels of relevant security architecture, the mandatory and systematic implementation of generally accepted requirements that currently in place to build reliable and secure information systems. It is important to implement complex, systemic and architectural solutions with the aim of their complete and comprehensive implementation. Analyzing and improving approaches to addressing security issues when building urban infor-mation systems based on IoT devices should be undertaken in the context of all levels of relevant security architecture, the mandatory and systematic imple-mentation of generally accepted requirements that currently in place to build re-liable and secure information systems. A new formal model of security subsystem of information technology platform for process support in urban resource networks formed on the basis of analysis of basic security characteristics of IoT-devices, built on their information systems and proposed by the authors information technology platform architecture is presented in this paper.

Keywords: Urban information system, IoT devices security, Security algorithms and protocols, Urban information system security approaches, Security attacks, Authentication and authorization procedures.

1 Introduction

Despite the prevalence and increasing popularity of integrated in different information systems sensors and meters that function as constituents of urban environments, im-

plemented as concept-oriented IoT devices, many of them have insufficiently implemented security mechanisms [1]. Due to the scarcity of computing resources and power consumption of IoT devices, their long life service and the unreliability of communication channels, classical security approaches of such profile systems are difficult to implement. Currently, many urban-integrated IoT devices operate under different operating systems and are implemented in a wide range of hardware configurations. This, in turn, complicates the formation of common standard communication and data exchange protocols. The lack of unified standards of communication and various hardware and software platforms of IoT-devices manufacturers complicate the processes of building secure municipal systems, which raises additional concerns about the security and protection of software-hardware complexes and information networks formed on their basis.

As the concept of IoT is relatively new, addressing the issue of organizing and building security systems in smart cities IT projects is highly important area of research and pioneering innovation. Building high-tech and high-performance systems based on IoT technologies generates a number of specific original scientific tasks and problems that need to be solved and their results practically embodied. Such problems include the lack of communication reliability, the security of their respective environments, and the lack of security in data and privilege systems.

A group of researchers from Ternopil Ivan Puluj National Technical University and National University "Lviv Polytechnic" is working on the development and practical implementation of information technology platform for process support in urban resource networks. The given platform is designed using sensors integrated on the basis of IoT-devices in urban resource networks. The construction of such type of information systems should be followed by the development, implementation and use of a wide range of different and diverse means and security measures. In this context, it is important to solve the problem concerning analysis of the basic security characteristics of IoT devices, built on their information systems and to construct the formal model of security subsystem of information technology platform to support the processes taking place in urban resource networks.

2 Analysis of the modern research state

The implementation of the concept of urban integrated IoT devices usually involves its presentation as a complex, distributed and heterogeneous system, generating a number of specific requirements to achieve the required level of security and privacy. The currently proposed Internet of Things security methods are essentially based on traditional known network security techniques. At the same time, we should aware that applying security mechanisms to IoT systems is much more complicated than in the case with traditional networks. In this case, the main factors of differences are the heterogeneity of devices, protocols, their scalability and the rapidly growing number of nodes. Application security issues implemented for processing and using data obtained from the urban environment using IoT devices, related in particular to the technical flaws of physical communication, heterogeneity of systems and datasets, limita-

tions on computing resources, the need for data privacy, large-scale of the systems, the feasibility of access rights demarcation and, in general, the lack of urban communities preparedness for security measures.

The consequences of IoT devices failure can be quite serious, particularly it can result in man-made disasters, pollution and destruction of ecosystems, etc. In paper [2], the authors provide a comprehensive analysis of current research in the field of IoT devices security, the analysis of trends and open questions. The state of research concerning the IoT devices security in smart cities and smart manufacturing projects has been analyzed by Jurcut, Pasika and Xu [3]. At the same time, the authors emphasize the importance of research, development and implementation of security technologies as the components of smart cities information systems. In paper [4] the authors presented a comprehensive analysis of IoT devices security threats and the formation of systematic measures for their elimination in smart cities. Hassija and others [5] provide a detailed analysis of security-related issues and highlight the set of threats sources in IoT applications. Information on security and privacy issues in relevant systems based on IoT technologies is provided in collective monograph [6]. While carrying out the investigations, the authors have analyzed each type of threat and reported it as a percentage for possible use of the Internet of Things technology. Currently developed and implemented security solutions for IoT devices are usually fragmented and partial, which in turn leads to the practical implementation of rather "dangerous" systems. One approach to this is to use the methods, tools, and security features used in building traditional security systems, but it is still unclear whether such "traditional" approach completely meets the needs and implements high level of security for IoT devices, since these systems have quite diverse and quite differentiated characteristics [7]. Nizzi in paper [8] proposed the method of performing the procedure of IoT devices addresses general shift.

In paper [1], the authors emphasize the need to develop secure communication protocols by proposing the use of Ethereum Blockchain concept. In paper [9] Rahman describes the use of Blockchain and IoT devices in providing financial and economic services in the smart city environment, and Sharifinejad in paper[10] proposes to use the Blockchain concept in the field of insurance services in smart cities. In monograph [11], the authors provide the systematic analysis of publications on improving the systems security based on IoT devices, particularly in information systems projects for smart cities. Sabrina in paper [12] proposed the architecture that uses "smart" contracts and public Blockchain to control information resources access of organizations and structural units of municipal government in the smart city.

A number of publications highlight the development of software-algorithmic complexes using IoT-platforms in smart cities information systems. Particularly, Badii [13] provides information about the framework that integrates different sources of information, consolidating data flows in innovative services and providing an adequate level of security based on the European Commission GDPR [14]. In paper [15], the authors present and analyze the architecture of the information technology platform formed using GDPR guidelines, and in [16] Waheed and Shafi consider the use of effective security framework to implement information systems projects in the smart cities. In paper [17], Waraga analyzes the processes of the open source IT plat-

form implementation to identify the vulnerabilities of networks and communications of integrated IoT devices in the urban environment.

3 Basic properties and characteristics of IoT devices and information systems based on them

IoT (Internet of Things) is a promising information technology aimed at building innovative information systems with high-tech features and parameters [18], which are used particularly to improve the quality of urban communities life by creating new software-algorithmic applications that make it more comfortable and facilitate their daily activities [4]. In this case, IoT devices have a number of the following generalized characteristics and properties:

- Limited energy and resources. The vast majority of IoTs are endowed with limited computing resources to minimize energy consumption and reduce the cost of equipment.
- Sensors. Sensors are one of the IoT device key elements, that are used to track changes in the environment and capture relevant datasets.
- Adaptability and self-configuration. Purpose-based IoT devices are typically configured to perform a number of operations to minimize human intervention, and as a consequence, can use automatic configuration algorithms and software update procedures.
- Unique device identity. In networks built on IoT-based devices, each object is identified using a unique identifier, which is typically the use of unique IP address.
- Integrated interfaces. Most of IoT devices have interfaces that allow users to perform setup, information retrieval, and remote control operations.
- Smartness. The implementation of complex software algorithmic applications in IoT devices confers them to some extent with the features of "smartness". These smart tools allow you to integrate IoT devices with other communications equipment and to implement effective "smart" decision-making procedures.

By implementing IoT information technology into urban information systems, the corresponding generalized cloud computing model and corporate concept for using IoT devices should be pre-formed [19]. When building urban information systems based on them, a number of their specific characteristics should be considered, particularly:

- Dynamic environment. IoT devices allow the dynamic integration of a wide range of urban assets without the need to define the boundaries of relevant IoT networks.
- Heterogeneity. One of the main features of urban information systems built using the Internet of Things technology is the ability to connect multiple types of devices with different sets of characteristics, such as operating systems, platforms, communication protocols and the corresponding range of functionality.
- Large amounts of data. Currently, the total number of IoT devices installed in the information systems is estimated as billions of pieces. In the process of their opera-

tion, these devices generate data collections, which in many cases can be attributed to the Big Data concept. This raises the need for resources and effective means of implementing the device interaction processes, control, storage of generated data large volumes, their interpretation and analytical processing.
- Context dependency: On the IoT platform, a large number of sensors integrated into the urban environment that implement the processes of selecting, storing and transmitting information that needs to be processed depending on the context.

System complexity. Information systems construction using IoT devices typically contain a large number of heterogeneous objects with a variety of hardware and software characteristics, which significantly complicate the implementation of management processes under severe constraints on computing resources, power consumption, and response time.

4 Security of urban information systems based on IoT devices

The given diversity of IoT devices and the wide range of communication protocols, interfaces and services used in urban information systems, makes it difficult to implement traditional security solutions and methods of well-known networked information technologies effectively [20]. Typically, traditional network security measures may not be sufficient in such cases. In order to confirm and to support the reasoning of the approach proposed by the authors, the features of one IT project implementation to ensure the efficient management of urban resource networks are considered by the team of researchers from the Ternopil Ivan Puluj National Technical University and Lviv Polytechnic National University. As a prototype, the methodology proposed by the open-source software development community known as the Open Web Application Security Project (OWASP) [21] was chosen for the creation of specifications and the construction of the conceptual secure information technology platform framework to support processes occurring in urban resource networks. Attacks listed in OWASP can be targeted on three layers of IoT systems, in particular, layers of hardware, communications and interfaces or services. Therefore, the implementation of measures to improve the IoT devices security and systems should cover the security architecture in all these layers comprehensively (see Fig. 1).

The solution of security problems in information systems built on IoT devices is relevant in the context of all three layers presented in the architecture in Fig. 1. For example, the absence of encryption algorithms for transport protocols causes the communication processes between the IoT device and cloud services, IoT device and gateway, IoT device and mobile applications, various IoT devices, etc. to be unsafe.

Much of the threats are due to IoT devices access through inadequate or ineffective authentication and authorization procedures. Modern IoT systems use protocols that support authentication, including MQTT, DDS, Zigbee, and Zwave. However, in many cases, the means of authentication offered by manufacturers are not sufficient to avoid the precedents of data hijacking at the communications level.

Unsecured network services do not allow the detection of malicious activities, or the threats of unauthorized intervention into IoT network and the dissemination of

"harmful" data. Currently, authentication is one of the popular methods of implementing secure communications at the network level. Despite the limitations of individual IoT devices computing capabilities, some researchers propose to implement IPSec in the IoT environment using a separate adaptation layer [22]. There is also ongoing research aimed at creating an easy authentication system based on public key management methods [23].

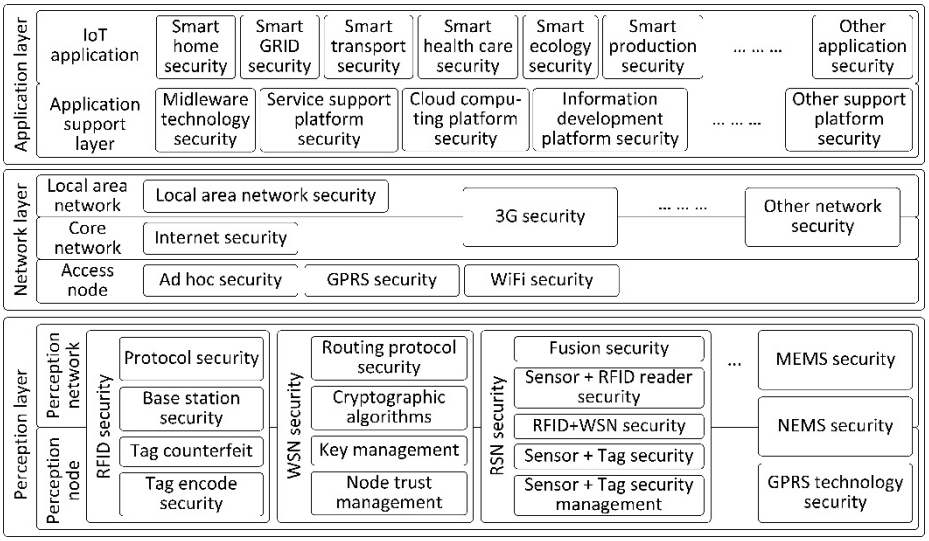

Fig. 1. IoT systems Security architecture

Security threats are caused by the rigid configuration of the same access codes for many IoT devices, which makes the credentials easy to change. It should be noted that the low level of IoT devices physical security results in the high vulnerability of hardware to malicious interventions and influences. The main difficulties in encryping IoT devices are their relative simplicity, limited availability of computing resources, and reduced usability. Therefore, it is necessary to develop "light" and efficient encryption algorithms for IoT devices in order to ensure privacy and security while using them. A separate object of cyber attacks in urban IoT systems is the software-algorithmic layer, which elements are implemented using cloud interfaces and services. Cloud gateways must be equipped with security controls to avoid malicious influences on their configurations change. Biometric and multi-level authentication tools can be effectively used to control access to cloud systems.

In addition to implementing the security policy for individual IoT devices, the general requirements applied in the context of arbitrary information systems built with their use [15] should be considered, particularly:

- Consideration of heterogeneity of characteristics of sensors, actuators and computing means of IoT devices.
- “Shading” of data storage and management of IoT devices.

- Routing and data transfer security when performing fog computing based on IoT devices.
- Abstractness of applications and IoT devices when interacting with IoT directories, data and knowledge bases.
- Scalability of cloud services for IoT devices, Context Brokers, Container, IoT applications.
- Abstracting of software-algorithmic tools for data analytical processing from personalization of datasets and minimization of personalized analytical results presentation.
- Abstract procedures for using contextual filtering of data from personalizing datasets.
- Providing security of dashboards, software-algorithmic means for presentation, visualization, and data analytical processing with Web-Socket support.

5 Increasing the security level of the information technology platform that support processes occurring in smart city resource networks

Urban resource networks are categorized as critical infrastructure systems and therefore require improved reliability and security characteristics [24]. The architecture of the information technology platform for supporting processes occurring in urban resource networks based on integrated IoT devicesuse, is presented in paper [25]. The group of researchers from Ternopil Ivan Puluj National Technical University and National University "Lviv Polytechnic" is working on the design and practical implementation of the given information technology platform.Work on the practical testing of the specified information technology platform that support processes occurring in the smart city resource networks [26] is carried out on the basis of six-layer architecture (see Fig. 2), which includes: sensor layer, network layer, acquisition layer, storage, processing and visualization layers. The sensorics layer, in turn, is conventionally divided into three sublayers. The sublayer of sensors contains water, gas, electricity and heat meters integrated into relevant smart city resource networks.

The next three layers are constructed on the cloud-based concept of building the smart city IT environment. The data sets generated at this layer are taken to the next level and stored in a distributed scalable data storage, which generates for each IoT device the corresponding set of information entities that are grouped in thematic databases.

At the data processing layer the appropriate analytical and data processing tools used to interact with the billing systems, mobile and web applications, and interfaces placed at the data visualization level are grouped. Currently, the authors are working on specification and development of security methods and tools for all levels of information technology platform presented in Fig. 2. Especially, security solutions according to the levels presented in Fig. 1, are divided into three layers: perseption security, network security and application security. Security tools used for the smart city cloud platform are distinguished as a separate element.

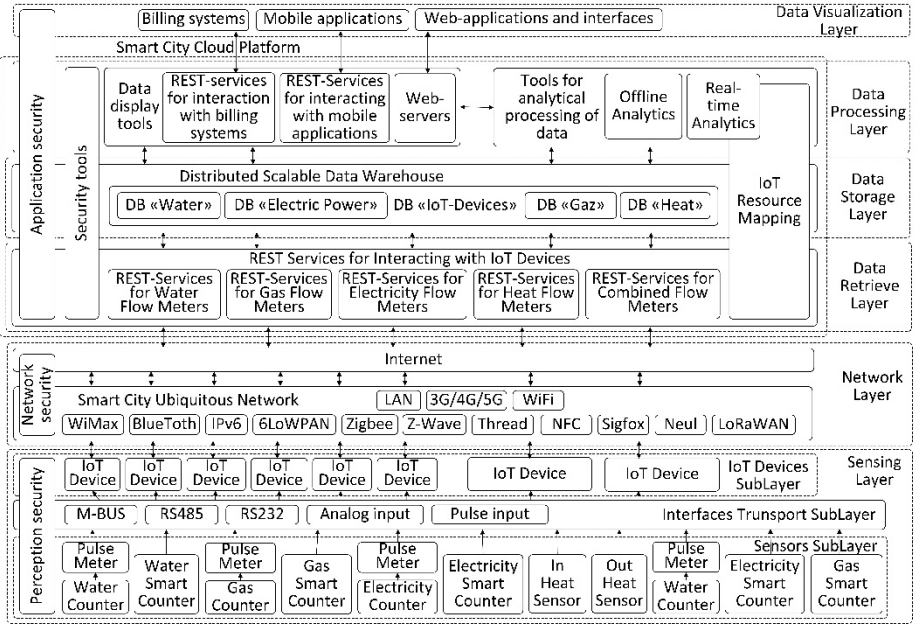

Fig. 2. Architecture of information technology platform that support processes occurring in smart city resource networks

In the process of the modern smart city IT projects implementation, a wide variety of vulnerable situations used by attackers to harm physical devices objects, peoples, urban groups or communities is formed. Possible security threats to smart city information systems require detailed analysis and elaboration, as they can significantly affect both the productivity and efficiency of urban services and the overall viability of the city as the center of human civilization space [4]. In such projects, particular attention should be paid to distiguishing such security factors and situations, such as:

- Equipment safety. Sensors integrated with physical objects based on IoT devices are the starting point of any cyber attack. Therefore, checking and ensuring the physical security of equipment can prevent many of these threats. The solution to this problem is somewhat complicated by the lack of IoT devices hardware standardization. Insufficient physical security can lead to theft, damage, or manipulation of IoT devices without altering basic functionality for the purpose of transmitting false data or runing relevant applications on critical systems that are urban resource delivery networks.
- MITM Attack. In the critical infrastructure systems, an attacker can artificially introduce additional "harmful" nodes between communication elements in order to steal transmitted data. MITM attack is used to replace key elements by using DoS attack on node elements in order to deny servicing of connected IoT devices and their further replacing by an artificially created "malicious" node.

- Datasets theft. Data created in smart city infrastructure complexes, in case of insufficient security, can be used to gain by the intruder a variety of personal information, which can be used for fraudulent transactions and thefts or interference in the privacy of citizens and visitors of the city.
- Great field attack. The scale of ubiquitous smart city networks creates a vast field for a wide range of cyberattacks. As smart city projects are implemented on the basis of many information systems and numerous integrated IoT devices used to manage a variety of services, any of the elements is potentially vulnerable and can be subject to cyberattack. Attacking only one element can pose a significant threat to the entire network or to information system at whole.
- Software-algorithmic errors. These kinds of errors can have a critical and unpredictable impact on individual devices as well as on software-algorithmic complexes or urban systems at whole, and their cost can be prohibitively expensive.

The development and effective implementation of a wide range of multi-type security mechanisms for smart city information systems is a prerequisite for the implementation of innovative services using modern IT and, in particular, those IoT concept based that focused on improving the quality of individual townspeople life and urban communities [4]. Information technology security solutions, methods and tools used in the processes of modern safe smart cities formation include:

- Developing means to improve the physical security of the equipment. These include methods for detecting, monitoring, and fast responding to physical damage or intrusion in both urban-integrated IoT devices and communications equipment of urban communications networks.
- Mutual authentication. Effective authentication mechanisms and procedures must be implemented for the various types of IoT devices connected to ubiquitous urban networks at all stages of data exchange. This, in turn, will confirm the identity of IoT devices and communications equipment and provide an adequate level of protection for the data transmission and reception against malicious cyber attacks.
- Operational monitoring and analysis of information systems security elements. This information should be promptly collected and processed to effectively identify potential security breaches and respond promptly to potential threats. Once the threats have been identified, appropriate operational response procedures based on a systemic security policy should be implemented.
- Data integrity and confidentiality. Smart city information systems projects use IoT-collected data to improve the quality of provided services and the living standards for the locals. The data collections must have a high level of accuracy and reliability. For this purpose, comprehensive data integrity measures should be applied to prevent manipulation during the transmission, storage, analytical processing and submission processes. Security measures, methods and tools should be used comprehensively and systematically in the process of building and operating urban information systems, in order to avoid the disclosure of sensitive or critical information.

6 The model of security subsystem of the information technology platform for process support in urban resource networks

Us provide the generalized information concerning the architecture of the information technology platform, security factors and information security solutions as the formal description of the security subsystem model of the information technology platform for process support in urban resource networks in the form of a tuple:

$$S_{res} = \left(T, P, FS_i^{IoT}, MZ^{IA}, Z^{MA}, R\right). \quad (1)$$

Components S_{res} are:

T – the set of threads identified for each of the security factors listed in the previous paragraph, particularly:

$$T = \left\{T_{Hardware}, T_{MITM\_Attak}, T_{Data\_Theft}, T_{Big\_Scale}, T_{Program}\right\} \quad (2)$$

In turn, each of these listed elements is also a set, for example, $T_{Hardware}$ is a set of threats for physical equipment, which includes:

$$T_{Hardware} = \left\{T_{Hardware}^1, ..., T_{Hardware}^N\right\} \quad (3)$$

P is a set of protocols, rapid response for each element from the threats set T.

FK^{IoT} is plurality of sets of functional security components integrated for each from the plurality of IoT devices types

$$IoT = \{IoT_1, ..., IoT_M\} \quad (4)$$

For particular $I = \overline{1, M}$ type of IoT device:

$$FK^{IoT_I} = \left\{device_I, service_I, network_I, cloud_I, storage_I, dataset_I, use_I\right\} \quad (5)$$

MZ^{IA} is a set of methods, mechanisms and means for entities identification:

$$MZ^{IA} = \left\{MZ_{IoT}^{IA}, MZ_{Services}^{IA}, MZ_{Servers}^{IA}, MZ_{Users}^{IA}\right\} \quad (6)$$

Z^{MA} are security monitoring and auditing tools, which include a set of tools for each of the levels of the of the information technology platform architecture (see Fig. 2) and integrated monitoring and auditing tools:

$$Z^{MA} = \left\{Z_{Perseption}^{MA}, Z_{Network}^{MA}, Z_{Application}^{MA}, Z_{Security\_tools}^{MA}\right\} \quad (7)$$

R is a set of access rights and user privileges, which includes group policies, personal and calculated sets of access rights and privileges:

$$R = \left\{ R_{Group\_policy}, R_{Personal\_user\_right}, R_{Calculated\_user\_right} \right\} \quad (8)$$

7 Conclusions and future investigation

At present the information technologies formed with the use of IoT-devices are being dynamically developed, making it possible to implement new software-algorithmic complexes and urban services constructed on their basis. However, there is no system basis and comprehensive vision of the conceptual problem solution concerning the development of safe urban systems with increased complexity among the manufacturers and suppliers of IoT devices In this paper the authors proposed a new formal model of the security subsystem of information technology platform to support the processes occurring in urban resource networks. This model can be used by municipal authorities, developers of relevant information systems and services, resource providers and manufacturers in order to plan the security strategy while using IoT devices. The proposed model is constructed on the basis of the analysis of a wide range of known solutions and on the basis of information obtained during development and practical implementation of the relevant information technology platform.

In the future, we are going to develop the conceptual framework which can be used for formal analysis, description and determination of the general security state and knowledge level concerning the creation of appropriate information technology platforms focused on the smart city concept.

References

1. Reilly E, et al (2019) A smart city iot integrity-first communication protocol via an ethereum blockchain light client. Proceedings of the International Workshop on Software Engineering Research and Practices for the Internet of Things (SERP4IoT 2019). Marrakech, Morocco
2. Hassan WH (2019) Current research on Internet of Things (IoT) security: A survey. Computer Networks 148, pp 283–294
3. Jurcut AD, Pasika R, Xu L (2020) Introduction to IoT Security. IoT Security: Advances in Authentication, pp 27–64
4. Atlam H, Wills G (2020) IoT Security, privacy, safety and ethics. Digital Twin Technologies and Smart Cities. Springer, Cham, pp 123–149
5. Hassija V, et al (2019) A survey on IoT security: application areas, security threats, and solution architectures. IEEE Access 7: 82721-82743
6. Devarakonda S, Malka N, Azeem M (2019) Critical issues in the invasion of the Internet of Things (IoT): Security, privacy, and other vulnerabilities. Handbook of Research on Big Data and the IoT. IGI Global, pp 174–196
7. Oliveira A (2019) IoT SECURITY ASSESSMENT. Diss. Universidade de Coimbra
8. Nizzi F, et al (2019) IoT security via address shuffling: the easy way. IEEE Internet of Things Journal 6.2: 3764-3774

9. Rahman Md A, et al (2019) Blockchain and IoT-based cognitive edge framework for sharing economy services in a smart city. IEEE Access 7: 18611-18621
10. Sharifinejad M, Ali D, Javad R (2020) BIS-A Blockchain-based Solution for the Insurance Industry in Smart Cities. arXiv preprint arXiv: 2001.05273
11. Ekramifard A, Amintoosi H, Hosseini Seno A (2019) A Systematic Literature Review on Blockchain-Based Solutions for IoT Security. The 7th International Conference on Contemporary Issues in Data Science. Springer, Cham
12. Sabrina F (2019) Blockchain and Structural Relationship Based Access Control for IoT: A Smart City Use Case. 2019 IEEE 44th Conference on Local Computer Networks. IEEE
13. Badii C, et al (2020) Smart City IoT Platform Respecting GDPR Privacy and Security Aspects. IEEE Access 8: 23601-23623
14. General Data Protection Regulation. GDPR, https://gdpr-info.eu/
15. Badii C, et al (2019) Privacy and security aspects on a Smart City IoT Platform. Proceedings of the 16th IEEE International Conference on Advanced and Trusted Computing, ATC Leicester, UK
16. Waheed A, Shafi J (2019) Efficient Cyber Security Framework for Smart Cities. Secure Cyber-Physical Systems for Smart Cities. IGI Global, pp 130–157
17. Waraga OA, et al (2020) Design and implementation of automated IoT security testbed. Computers & Security 88: 101648
18. Duda O, Kunanets N, Matsiuk O, Pasichnyk V (2018) Information-Communication Technologies of IoT in the "Smart Cities" Projects. CEUR Workshop Proceedings, vol. 2105, pp 317–330
19. Arun A (2020) Architecting IOT for Smart Cities. Smart Cities in Application. Springer, Cham, pp 141–152
20. Pasichnyk V, et al (2018) Telecommunication Infrastructures for Telemedicine in Smart Cities. IDDM 2018 Informatics & Data-Driven Medicine, vol. 2255, pp 256–266
21. Open Web Application Security Project, OWASP, https://owasp.org/
22. Bhattacharjya A, et al (2020) CoAP – application layer connection-less lightweight protocol for the Internet of Things (IoT) and CoAP-IPSEC Security with DTLS Supporting CoAP. Digital Twin Technologies and Smart Cities. Springer, Cham, pp 151–175
23. Alkatheiri MS, Abdur RS, Satish A (2020) Physical Unclonable Function (PUF)-Based Security in Internet of Things (IoT): Key Challenges and Solutions. Handbook of Computer Networks and Cyber Security. Springer, Cham, pp 461–473
24. Little R, et al (2020) CLARC: An Artificial Community for Modeling the Effects of Extreme Hazard Events on Interdependent Civil and Social Infrastructure Systems. Journal of Infrastructure Systems 26.1: 04019041
25. Duda O, Kochan V, Kunanets N, Matsiuk O, Pasichnyk V, Sachenko A (2019) Data Processing in IoT for Smart City Systems. In: Proc. 10th IEEE Intern. Conf. on. Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2019), Metz, pp 96–99
26. Duda O, Kunanets N, Matsiuk O, Pasichnyk V (2018) Cloud-based IT Infrastructure for “Smart City” Projects. In: Dependable IoT for Human and Industry: Modeling, Architecting, Implementation. River Publishers, pp 389–410