Classification of Security Risks in the IoT Environment

Conference Paper · October 2015

DOI: 10.2507/26th.daaam.proceedings.102

CITATIONS
19

READS
1,522

3 authors:

Ivan Cvitić
University of Zagreb
28 PUBLICATIONS **56** CITATIONS
SEE PROFILE

Miroslav Vujić
University of Zagreb
25 PUBLICATIONS **61** CITATIONS
SEE PROFILE

Sinisa Husnjak
University of Zagreb
31 PUBLICATIONS **96** CITATIONS
SEE PROFILE

CLASSIFICATION OF SECURITY RISKS IN THE IOT ENVIRONMENT

Ivan Cvitić, Miroslav Vujić, Siniša Husnjak

University of Zagreb, Faculty of Transport and Traffic Sciences, Vukelićeva 4, 10000 Zagreb, Croatia, EU

Abstract

The concept of Internet of Things (IoT) is based on a layered architecture. Each of the layers includes the application of a range of diverse technologies for the data transmission, processing and storage. This paper will explore the vulnerabilities and threats in IoT environment and protection methods that can be implemented within such an environment due to the hardware limitations of the existing equipment and technology used for data transfer. Based on the results of the research, classification of security risks of the architectures' particular layer, as well as security risks depending on the type of use of IoT concept will be proposed. The classification of risk will provide the opportunity to direct further research on the most vulnerable layers of the architecture and implementation of appropriate methods of protection, depending on the application of this concept. This research was conducted in order to provide accurate information for visually impaired people.

Keyword: AIDC; Internet of Things; Security architecture; Risk assessment; Data protection

This Publication has to be referred as: Ivan, C[vitic]; Vujic, M[iroslav] & Husnjak, S[inisa] (2016). Classification of Security Risks in the IoT Environment, Proceedings of the 26th DAAAM International Symposium, pp.0731-0740, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-07-5, ISSN 1726-9679, Vienna, Austria
DOI:10.2507/26th.daaam.proceedings.102

1. Introduction

The growing role of the Internet of Things (IoT) concept is proved by its application in the number of areas such as the development of smart cities, the management of energy resources and networks, mobility, transport, logistics, etc. The increase in the application and the importance of this concept results in an increasing number of diverse data being processed, stored and transmitted in different environments. The high level of complexity of the IoT concept and the use of Automatic Identification and Data Capture (AIDC) technologies increases the risk of compromising the basic principles of safety which is why this problem domain remains continuously investigated in the last few years. The main research question of this paper is which layer of the IoT architecture and what application of the IoT concept has the highest security risk. The aim of this research paper is to examine security aspects of a particular layer of the IoT architecture which will make the basis for the proposal of the risk classification in order to focus further research and development of appropriate protection methods of the most vulnerable layers. In addition, the risk classification will be carried out depending on the application of the IoT concept in various environments in order to implement appropriate methods of protection.

1.1. Previous research

According to [1], problems of security are classified according to the layers of the architecture of the IoT concept. Based on the security problems, the protection methods are listed and classified according to the architecture layers , but also according to the used technologies and in the dependence on the application environment of the IoT concept. Finally, the comparison of security problems within the IoT concept and traditional information and communication environment is made.

The use of Wireless Sensor Networks (WSN) in the concept of IoT is growing, and the problems of WSN security are discussed in a number of research papers [2, 3, 4, 5, 6]. In the research [7], the authors analyzed the application of WSN in a military environment in the function of providing services such as information about the presence of a moving vehicle, the detection targets and other events, depending on the defined mission. The paper has identified the threats aimed to compromise the nodes of the network, eavesdropping in order to analyze the network traffic, disabling of the base station and the impact on the data flow. The aim is to develop a new security architecture "SurvSec" intended for reliable recovery of the network functions after the impact on the security of the base station within a WSN.

In [8], the potential risk of conducting Denial of Service (DoS) attacks in the Wireless Body Area Networks (WBAN's) is recognized. Given the limited processing and the storage resources, the authors have noticed the existence of threats targeting the availability of data in such networks, and identified a Distributed Denial of Service (DDoS) attacks as a threat of the highest risk directly affecting the availability of users' (patients') data. Research has shown that the TCP SYN flooding type of DDoS attacks makes the greatest threat considering the fact that the 85% of DDoS attacks are based on the TCP protocol. Within the literature overview of the current problem areas, it was concluded that the protection methods against previously identified types of attacks contain many defects. Based on previously stated facts, the development of a framework for the detection, prevention and avoidance of such attacks is made in order to ensure continuity of the access to WBAN environment and maintenance of the required level of the quality of services.

The standard 802.14.5 (which make the basis of ZigBee data transfer technology) is often used in IoT environment. Advantages such as high autonomy, flexibility and price acceptability of implementation represent the negative side of this technology for security aspect. The vulnerabilities and protection methods of ZigBee technology are observed in [9].

Standard protection methods applicable to the perimeter of the information and communication systems, such as firewall, intrusion detection system and intrusion prevention system are not applicable in the IoT environment. The architecture making the basis of this concept has no clearly defined boundaries, which makes an additional security problem of network access control. The research [10] proposes a security model in IoT environment based on the use of Software Defined Network (SDN) architecture.

1.2. Research methodology and the limitations

This paper analyzes research of other authors in the field of the IoT concept security, as well as in the field of cloud computing, computer networks and AIDC technologies as component parts of IoT architecture. The synthesis of the collected data presents the new findings and the proposed classification of risk in IoT environment with an aim to provide a research direction for any further research on the safety critical layers of IoT architecture.

Risk classification of each layer is limited to a qualitative assessment due to lack of exact data. Although the risk assessment can be affected by numerous parameters, classification of risk depending on the application of the IoT concept in various environments is based exclusively on application growth of this concept in the time period 2013 - 2014. The problem considered in this paper is observed from the security risk approach as a fundamental protection component of all information and communication environment forms.

2. The architecture of IoT environment

IoT architecture concept is based on an open model using open protocols in order to support existing network protocols. Generic, layered architecture of IoT concept consists of four basic layers (perception layer, network layer, middleware layer and the application layer), shown by Figure 1 [11].

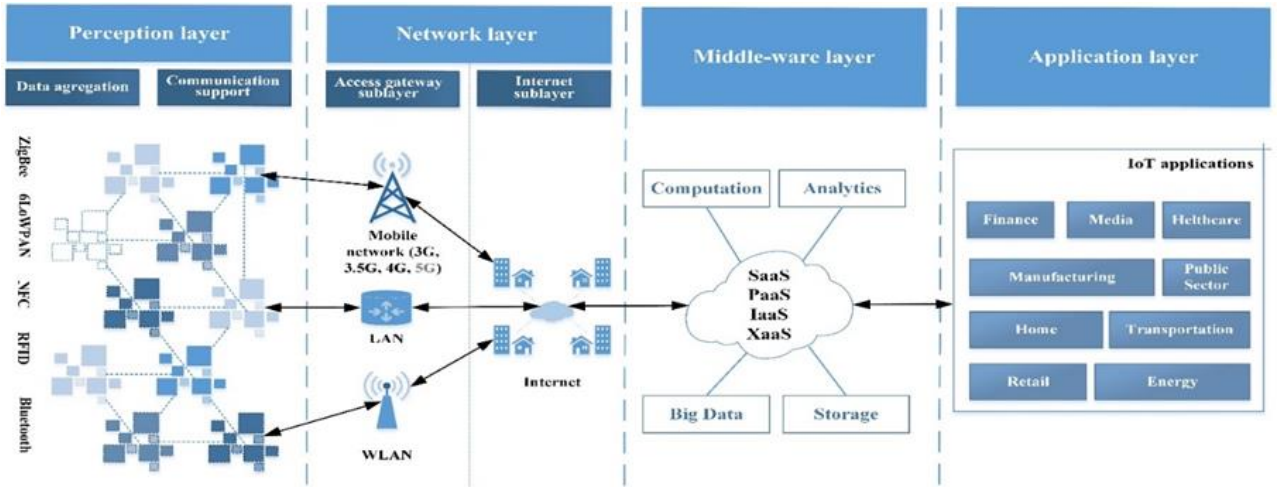


Fig. 1. Architecture of the IoT concept [11, 12]

According to [12] perception layer consists of two main functionalities, data collection and collaboration between the elements of the same layer. The network layer consists of two sublayers, access sublayer with the role of collecting the data from perception layer and sending it to the Internet sublayer. Internet sublayer is the backbone of IoT environment and its main task is the transfer of data to the next layer, middleware, a layer which perform the processes such as intelligent routing and the network address translation. Middleware layer is responsible for data collecting, its filtering, transformation and the intelligent processing most commonly with the use of cloud computing concepet. After processing, the data is passed to the application layer, which uses the given data in order to provide and present various services to the end user [1].

3. Security aspects of the IoT architecture layers

This chapter will present the security features of each layer of the IoT architecture with the focus on perception layer specific to the IoT environment. Until the development of IoT concept, networks of sensors are used in enclosed information and communication systems without Internet access. Within the IoT architecture, network, middleware and application layer make integral components of the classical information and communication environments, while the perception layer is present exclusively within the IoT environment.

3.1. Threats and the vurnabilities of the perception layer

Devices of the perception layer are often limited in terms of process and data storage resources, and the applied technologies (such as RFID/NFC, Bluetooth, ZigBee and 6LoWPAN) are being limited in data transsmision range and rate. Restrictions are imposed in order to achieve greater autonomy, reduce physical dimensions and increase the flexibility of such devices, but also to reduce the final cost of such devices.

Features/Technology	NFC	RFID	Bluetooth	ZigBee	6LoWPAN
Coverage Area	PAN	PAN	PAN	LAN	LAN
Topology	P2P	P2P	Star	Mesh/Star/Tree	Mesh/Star
Power consumption	Very Low	Very Low	Low	Very Low	Very Low
Speed	400 Kbps	400 Kbps	0,7 - 1 Mbps	250Kbps	250Kbps
Range	< 10 cm	< 3 m	5 - 30 m	10 - 300m	800 m

Table 1. Transmission technology features of the perception layer [13]

Basic features of each transmission technology, such as the coverage, topology, power consumption, data transmission rate and range, are shown in Table 1. Perception layer is specific in the IoT environments, opposed to the other layers which are in some form present in other information and communication environments.

3.1.1. Security aspects of RFID and NFC technology

Within the IoT environment, RFID technology is used mostly for the automated information exchange. Due to known security disadvantages of this technology there are a number of assumed threats. The lack of adequate authentication mechanisms in a number of RFID tags allows unauthorized access to their contents. Although the content of the tag is not easy to read, the unauthorized alteration of its content or its deletion is very possible. The attack on the availability of RFID tags can be carried out through a DoS attacks. DoS attack causes the failure of transmission of identification information stored in the tags. Threats against the confidentiality of the data include attacks such as tag monitoring with the use of an unauthorized reader which can result in the interception of sensitive information such as street addresses, phone numbers, and identification tags. Attacks on the data integrity are related to unauthorized tag cloning with the use of unauthorized readers which allow cloning in order to bypass implemented protection methods. In addition to these threats, environments using RFID technology are also vulnerable on eavesdropping, MitM attacks, spoofing, and others [6, 11].

NFC technology is different from RFID in used frequency range and connection topology. The technology is based on the principles and the relations between magnetism and the electricity, or on the principles of the inductive loop [14]. Although short-range, NFC technology is vulnerable to many threats such as eavesdropping, unauthorized manipulation of data and MitM attacks [15]. Although eavesdropping and MitM attack methods are considered less risky, these attacks are possible with the use of the expansion method of communication range up to 10 meters in the active communication mode and up to one meter in the passive communication mode [16, 17].

Threats	Method of protection	Technology	Description
Tag Cloning	Syncronized secrets method [18]	RFID	Synchronized secrets method that can detect cloning attacks and pinpoint the different tags with the same ID
Information leakage	RFID-Tate [19]	RFID	Light-weight identity protection and mutual authentication using Identity-based Encryption (IBE) method.
Eavesdropping, tag cloning	OTP authentication [20]	RFID	Method uses dynamic password and backend system authentication methods. It can effectively prevent the security vulnerabilities such as dictionary attacks, replay attacks, data eavesdropping and tags forgery.
Evesdropping, location tracking, replay attack, MitM, De-Syncronization Attack	VLFSR lightweight encryption function [21]	RFID	Security method is successful against the large scale of attacks on RFID. It can be used in design of secure RFID protocol with efficient hardware requirements to meet the demand of secure low-cost RFID systems or WSN.
Identity theft, information leakage	Conditional privacy protection method [17]	NFC	Proposed method can provide conditional privacy with less overhead, it can also hide user's identity, and its identity can be confirmed by the TSM (Trusted Service Manager).
Eavsdropping	Random key agreement method [16]	NFC	Practical and energy efficient key agreement method for duplex NFC.

Table 2. Threats and the protection methods for the RFID and NFC technology

Table 2 presents some of the developed methods applicable to the protection of RFID and NFC technology within the IoT environment. Methods have been developed taking into account the specifics, or disadvantages of RFID and NFC technology.

3.1.2. Security aspect of the Bluetooth technology

Bluetooth is a wireless communication technology for short-range communication. The technology enables the creation of Adhoc, piconet, network between two or more devices, and has implemented protection methods that are based on authentication and encryption. There are four modes of protection (Security mode 1, Security mode 2, Security mode 3 and Security mode 4). Mode 1 does not require authentication and encryption, mode 2 applies authentication and encryption exclusively for individual services such as data transfer, mode 3 forces authentication, and encryption before the connection with the device is established, and mode 4 uses a simple method of pairing with the aim of establishing security on the service level [22].

Type of threat	Threat level
Surveillance	*Low*: The primary function is to gather information on the use. If it's used alone it does not represent a major threat.
Range extension	*Low*: Provides the option of extending the range for ease of execution attacks. If it's used alone it does not represent a major threat.
Obfuscation	*Low*: The primary function is to hide the identity of the attacker. If it's used alone it does not represent a major threat.
Fuzzer	*Medium*: Communication breakdown caused by this threat usually does not cause much damage because the corresponding technology is not used for critical communication.

Sniffing	*Medium*: It is used for the extraction of unencrypted data traffic. Although some devices do not use encryption, most of the traffic is encrypted by default.
Denial of Service	*Medium*: Because the technology is not used for critical communications, DoS attacks do not cause any significant damage.
Malware	*Medium*: Transmission range supported by the technology limits the threat to a small number of devices.
Unautorized direct access (UDDA)	*High*: The purpose is an unauthorized collection of personal data.
MitM	*High*: All the data exchanged between two devices can be gathered by a third party.

Table 3. The threats intended for the Bluetooth tehnology [23]

The threat classification of the Bluetooth technology is presented in [23] where the threats are classified into nine categories. Each threat is different, therefore each one is assigned to a threat level category. Table 3 shows the intended threats for the Bluetooth technology and threat levels.

3.1.3. The security aspect of the ZigBee technology

The ZigBee technology plays an important role in the formation of WSN because of advantages such as low cost, high reliability, low complexity and variety of application in the IoT environment. The advantages of this technology are the autonomy, flexibility, scalability and low cost of the devices. Despite the offered advantages, a large number of security threats are oriented against specified data transmission technology [9].

Some of the known security threats of the ZigBee technology are the unauthorized traffic gathering, packet decoding and data manipulation. For example, unauthorized access to a sensor node within a ZigBee network gives access to the shared secret key of the network and thus the traffic within the network. In addition to known threats, a new threats appear, such as the sabotage of terminal devices in the ZigBee network with the purpose of the exhaustion of the battery capacity and the exploitation of the key exchange process [24].

3.1.4. The security aspect of the 6LoWPAN technology

IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) is a communication technology that enables connectivity of the hardware limited devices (sensors, actuators, etc.) onto IPv6 network through the IEEE 802.15.4 standard [25]. This communication technology has an increasing role in the IoT environment due to the high presence of devices with limited processing, memory, and the other features. This technology also has a large number of vulnerabilities and threats that have the potential of their exploitation.

Threat	Protection method	Description
Sybil Attack	Check on the number of instances of each node, check on the geographical location of nodes through distributed hash table (DTH).	-
Wormhole Attack	Markle tree authentication	The method serves to prevent attacks
Clone ID Attack	Check on the number of instances of each node, check on the geographical location of nodes through distributed hash table (DTH).	Methods aren't developed
Blackhole Attack	No evaluated technique available	-
DoS Attack	Intrusion detection system (IDS) solution i.e. SVELTE	-
Alternation and Spoofing Attack	VeRA (Version number and Rank Authentication)	Prevents misbehaving node from decreasing Rank Values for the purpose of the attack
Synchole Attack	IDS solutions, parent fail-over, rank authentication method	IDS and parent fail-over can detect, and the rank authentication method can avoid the attack
Selective Forwarding Attack	Hartbeat protocol	The method has the ability to detect attacks

Table 4. Threats and protection methods of the 6LoWPAN technology [25]

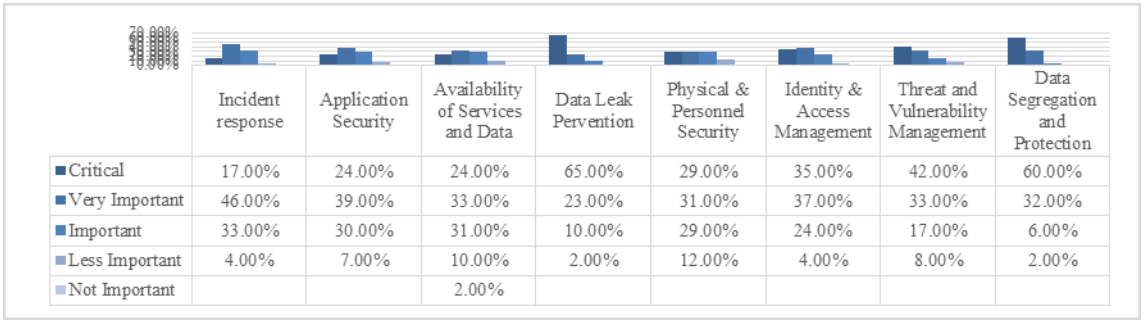
Table 4 provides the list of some of the possible attacks on 6LoWPAN supported devices. The table shows that for some attacks protection methods are not yet developed, or developed methods have the ability to detect but not to prevent the attacks [2].

3.2. Security aspect of the network layer

The network layer is not specific for the IoT environment, it is the backbone of every information and communication environment. Therefore, vulnerabilities and threats present in this layer are present in other environments which resaulting in frequently researched protection methods. The network layer of IoT concept consists of the access sublayer and the Internet sublayer. The access sublayer is used for the perception layer data acquisition, and for transferring the data to the core network, which forwards received data to the middleware layer. Typical security problems of this layer are traditional security problems, or communication networks security problems that affect confidentiality, availability and integrity of data. Although there are security concerns at this layer, protection methods are numerous and are well defined regarding other layers of the IoT concept.The most common security challenges are unauthorized network access, eavesdropping, confidentiality breaches, integrity violation, DoS attacks, MitM attacks, etc. [26].

3.3. Security aspect of the middleware layer

The middleware layer is based on cloud computing because of its benefits, such as delivery of computing resources as a service to end users, flexibility, scalability, etc. This makes it suitable for processing large amount of data collected on the perception layer and the presentation of processed data to end users through a variety of applications. Due to the rapid evolution and a high acceptance degree, this concept has a large number of threats and vulnerabilities that inherit the middleware layer of the IoT concept based on cloud computing [27].



	Incident response	Application Security	Availability of Services and Data	Data Leak Pervention	Physical & Personnel Security	Identity & Access Management	Threat and Vulnerability Management	Data Segregation and Protection
Critical	17.00%	24.00%	24.00%	65.00%	29.00%	35.00%	42.00%	60.00%
Very Important	46.00%	39.00%	33.00%	23.00%	31.00%	37.00%	33.00%	32.00%
Important	33.00%	30.00%	31.00%	10.00%	29.00%	24.00%	17.00%	6.00%
Less Important	4.00%	7.00%	10.00%	2.00%	12.00%	4.00%	8.00%	2.00%
Not Important			2.00%					

Fig. 2. The presentation of the threats in Cloud Computing [28]

According to research conducted in [28] and shown in Figure 2, a key security factors of cloud computing are identified. Those factors are related to the data leakage prevention (88% - critical / very important) and the data segregation and protection (92% - critical / very important). The fact that this layer accumulates all the data collected on the perception layer raises the issues of data security. An additional problem is the public or hybrid cloud computing model, where a single physical server can contain multiple virtual machines from different IoT service providers or even the presence of malicious users with the possibility to gain unauthorized access to other virtual machines and to manipulate stored data.

3.4. Security aspect of the application layer

Because of the variety of services placed within the application layer it is necessary to separate this layer from the rest of the IoT architecture and conduct its vertical classification according to risk of security breaches in relation to the market share of the IoT concept in a particular economic sector. The increase in the usage results in a greater number of applications and their instances, and thus a larger number of the existing devices and the transmitted data [29]. The end result is an increase of the potential attacks surface proportionally with the use of the IoT concept within the observed sector.

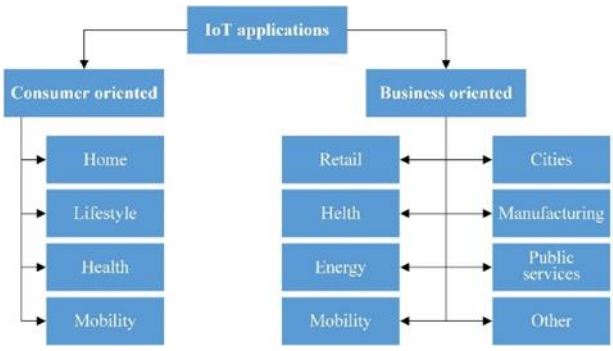


Fig. 3. Segmentation of the IoT applications [30]

In general, IoT application can be divided on the consumer and business-oriented applications. Additional segmentation of the IoT applications is shown in Figure 3.

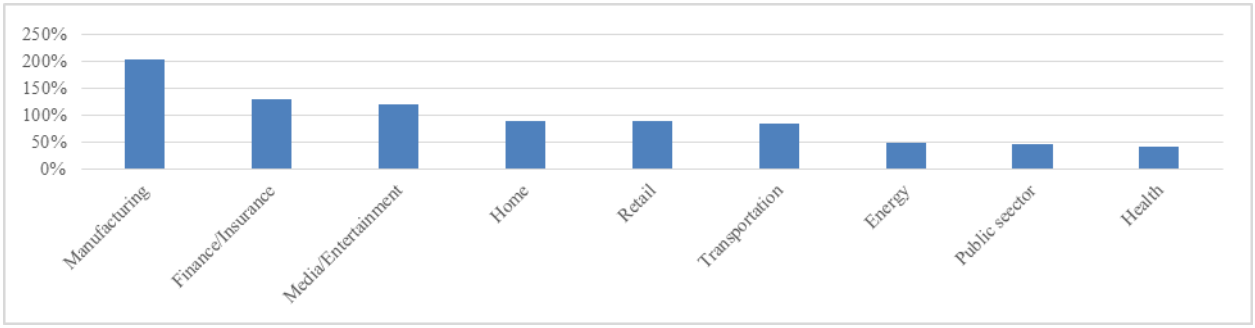


Fig. 4. The increase in the use of the IoT concept in a particular sector [31]

The annual growth in the use of the IoT concept according to the individual sectors can be seen from Figure 4. The largest increase in the use of the IoT concept was recorded in the manufacturing sector and amounted to 204%, followed by the financial sector with a 128%, multimedia sector with 120% and the home sector with 89% [31].

4. Risk classification of the IoT architecture layers

The key disadvantages of IoT concept according to the layers, as well as a description of these disadvantages are presented in Table 5. Besides the previously listed, the classification of each layer is presented from the highest (High) to the lowest (Low). The perception layer is classified with the highest security risk level due to very large hardware limitations that prevent the implementation of robust protection methods of the data collected, stored and transmitted at this layer. The risk level is also contributed by the heterogeneity of the devices within the perception layer which makes the establishment of security and the standardization of communication protocols more difficult

Access sublayer of the network layer is classified with the risk level Low-to-Medium due to the known disadvantages of wireless data transfer standards, as well as known threats in access networks. The advantage of this layer is the intensive research of the vulnerabilities and the continuous development of protection methods in the field of computer networks, due to the fact that the observed layer is an integral part of classic information and communication systems. An additional advantage is a support for robust protection methods assured from the devices used at the network layer. Internet sublayer of the network layer is classified with the risk level Low due to the extremely complex extraction of data transmitted from the access layer to the middleware layer. Threats that can exploit the vulnerabilities in routing protocols and publicly available routers are various forms of DDoS attacks that can disrupt the availability within the IoT environment.

Layer		Risk level	Disadvantages	Description
Perception		High	Physical characteristics of devices	Small dimensions require installation of hardware with even smaller dimensions and limited possibilities
			Price of device unit	The low price of the device results in the implementation of low-cost components of limited possibilities
			Physical exposure	Great number of devices located in the real environment is often difficult to protect against physical impact and an unauthorized manipulation
			Energy requirements	Devices have to satisfy high demands which results in the implementation of energy-saving components of limited possibilities
			Wireless communication	The use of the air as a data transmission medium allows unauthorized and simple data collection and the analysis of traffic that is often unencrypted or, because of the limited hardware capabilities, encrypted using weak cryptographic methods
			Implementation of security methods	Previously mentioned restrictions prevent the implementation of more robust methods of protection applicable to traditional information and communication environments
			Heterogeneity	A large number of devices using different transmission technology make it difficult to establish standard protocols and protection methods
Network	Access sublayer	Low-to-Medium	Application of the wireless communication technologies	The use of the air as a data transmission medium allows unauthorized and simple data collection and the traffic analysis
			Convergence of multiple users / devices at a single point	Due to connection of multiple devices in a single point (switch / hub), that point may be exploited for the implementation of a large number of attacks (eavesdropping, MitM, DoS, etc.).
	Internet	Low	Routing	OSPF, BGP, and other routing algorithms have flaws that can be

	sublayer		exploited for the purpose of security breach
Middleware	Medium	Publicly exposed routers	May be the target of the attacks such as DDoS
		High penetration in the number of users	One cloud computing service provider manages the data of a large number of private and business users which raises the issue of data segmentation, privacy, confidentiality, and similar.
		Low level of maturity of the technology	The rapid development of services based on cloud computing in recent years raises the risk due to insufficient research and the lack of protection methods
		Ability to set a large number of users classes on a single physical machine	Identified vulnerabilities of virtualization whose exploitment can causesimultaneously damage to a large number of users

Table 5. Risk classification of the IoT architecture layers

Middleware layer is classified with the Medium security risk level. The reasons are a large number of users and the data to be stored and processed within the layer, as well as the known vulnerabilities of virtualization whose exploitation can cause extensive simultaneous damage to a large number of users. Cloud computing is the current issue in the last ten years, and services based on this concept evolve rapidly, although there are still many shortcomings and possible threats.

Figure 5 presents the risk classification of the IoT architecture layers, based on Table 5. In addition, it presents the risk classification for the use of the IoT concept in various environments according to the increase of the use of IoT concept in a particular environment, as presented through Figure 4. According to the presented data the largest increase in the use of IoT concept relates to the manufacturing sector (204%), followed by the financial sector (128%) and the multimedia sector (120%), which is the reason for this sectors of the IoT concept to be classified as High security risk level. Sectors house (89%), sales (88%) and transport (83%) are classified as Medium security risks level, while energy (49%), public (46%) and healthcare (40%) sectors are classified as Low security risk level.

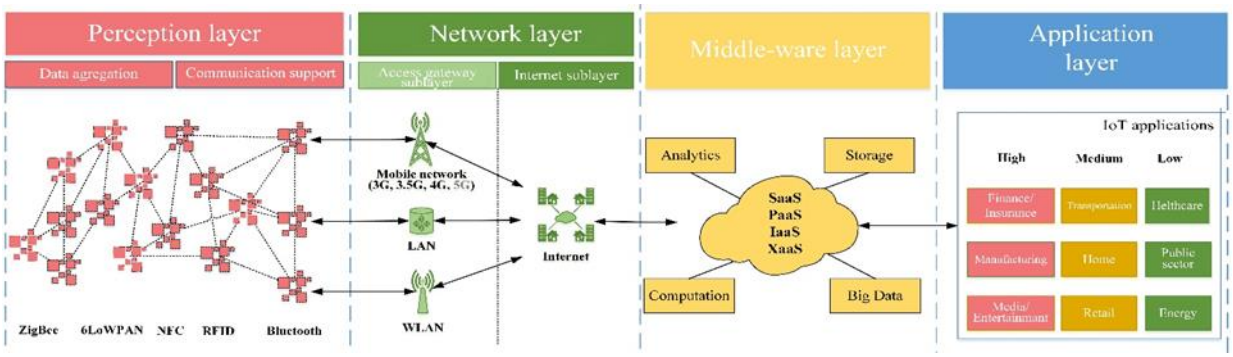


Fig. 5. Presentation of the risks of the IoT architecture layers

An example of the importance of implementing appropriate protection methods can be seen in the application of the IoT concept for guiding the visually impaired people through the traffic network [32, 33, 34]. Detection of user's movement is performed by means of RFID and NFC technology, what makes the basis for the user informing about his location at the crossroad. User identification information must be transmitted in a secure manner to prevent the unauthorized disclosure or manipulation. Feedback to the user must be accurate, reliable and protected against unauthorized manipulation that could endanger the safety of users within the traffic network.

5. Conclusion

The concept of IoT represents the evolution of the Internet and its appliance is continuously growing. According to estimates, by means of this concept 50 billion devices will be connected by 2020 which places heavy demands and challenges in maintaining the required safety level of such an environment.

This paper has analyzed the security aspects for each layer of the IoT architecture, and based on that, the proposal of risk classification of the IoT architecture layers has been made. In addition, the paper proposes the security risk classification of the use of IoT concept depending on its appliance.

By the analysis of security vulnerabilities, it was concluded that the biggest security risk is a perception layer of the IoT architecture due to the specific limitations of devices and the transmission technology used at this layer, followed by the middleware layer based on cloud computing and inherited vulnerabilities of that concept. The highest level of risk of the IoT concept application was determined for the financial, manufacturing and multimedia sector due to the largest increase of its usage in the period 2013 - 2014.

The results presented in this research provide new knowledge of security risks in the IoT environment. They are based on synthesis of previous research results and offers an opportunity to focus development of future protection methods on most vulnerable layers of IoT architecture.
Future research will be directed toward deficiencies and vulnerabilities of communication technologies on the perception layer of IoT concept and the possibility of implementing appropriate data protection methods.

6. References

[1] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, Security of the Internet of Things: perspectives and challenges, Wireless Networks, 2014, vol. 20, no. 8, pp. 2481–2501.
[2] P. Nandu and N. Shekokar, An Enhanced Authentication Mechanism to Secure Re-programming in WSN, Procedia Computer Science, 2015, vol. 45, pp. 397–406.
[3] D. P. Singh, R. H. Goudar, and M. Wazid, Hiding the Sink Location from the Passive Attack in WSN, Procedia Engeneering, 2013, vol. 64, pp. 16–25.
[4] T. Sheltami, An enhanced energy saving approach for WSNs, Procedia of Computer Science, 2013, vol. 21, pp. 199–206.
[5] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, Security, Privacy and Trust in Internet of Things: The Road Ahead, Computer Networks, 2015, vol. 76, pp. 146–164.
[6] T. Borgohain, U. Kumar, and S. Sanyal, Survey of Security and Privacy Issues of Internet of Things, International Jurnal of Advanced Network Applications, 2015, vol. 6, no. 4, pp. 2372–2378.
[7] M. H. Megahed, D. Makrakis, and B. Ying, SurvSec: A New Security Architecture for Reliable Network Recovery from Base Station Failure of Surveillance WSN, Procedia of Computer Science, 2011, vol. 5, pp. 141–148.
[8] R. Latif, H. Abbas, and S. Assar, Distributed Denial of Service (DDoS) Attack in Cloud- Assisted Wireless Body Area Networks: A Systematic Literature Review, Jurnal of Medical Systems, 2014, vol. 38, no. 11, pp. 1-10.
[9] W. Razouk, G. V. Crosby, and A. Sekkaki, New Security Approach for ZigBee Weaknesses, Procedia Computer Science, 2014, vol. 37, pp. 376–381.
[10] F. Olivier, G. Carlos, and N. Florent, New Security Architecture for IoT Network, Procedia Computer Science, 2015, vol. 52, pp. 1028–1033.
[11] M. Farooq, M. Waseem, A. Khairi, and S. Mazhar, A Critical Analysis on the Security Concerns of Internet of Things (IoT), International Jurnal of Computer Applications, 2015, vol. 111, no. 7, pp. 1–6.
[12] L. Zheng, H. Zhang, W. Han, and X. Zhou, Technologies, Applications, and Governance in the Internet of Things, in: O. Vermesan and P. Friess (Eds.), Internet of Things - Global Technological and Societal Trends From Smart Environments and Spaces to Green ICT, River Publishers, 2011, pp. 141–175.
[13] D. Atkinson and K. Karimi, What the Internet of Things (IoT) Needs to Become a Reality, Freescale Semicoductor Inc. 2014.
[14] D. Zupanovic, Implementation Model for Near Field Communication in Croatian Ferry Ticketing System, 25th DAAAM International Symposium on Intelligent Manufacturing and Automation, DAAAM 2014, 2015, pp. 1396–1404.
[15] N. A. Chattha, NFC - Vulnerabilities and Defense, Conference on Information Assurance and Cyber Security (CIACS), 2014, no. 1, pp. 35–38.
[16] R. Jin, X. Du, Z. Deng, K. Zeng, and J. Xu, Practical Secret Key Agreement for Full-Duplex Near Field Communications, IEEE Transaction on Mobile Computing, 2015, vol. 1233, pp. 1–16.
[17] H. Eun, H. Lee, and H. Oh, Conditional Privacy Preserving Security Protocol for NFC Applications, IEEE Transaction on Consumer Electronics, 2013, vol. 59, no. 1, pp. 153–160.
[18] M. Lehtonen, D. Ostojic, A. Ilic, and F. Michahelles, Securing RFID Systems by Detecting Tag Cloning, in: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2009, pp. 291–308.
[19] M. F. Sadikin and M. Kyas, RFID-Tate : Efficient Security and Privacy Protection, 5th International Conference on Information, Intelligence, Systems and Applications, IISA 2014, 2014, pp. 335–340.
[20] C. H. Huang and S. C. Huang, RFID Systems Integrated OTP Security Authentication Design, 2013 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference, APSIPA 2013, 2013, pp. 1–8.
[21] J. Garcia-Alfaro, J. Herrera-Joancomartí, and J. Melià-Seguí, Security and Privacy Concerns About the RFID Layer of EPC Gen2 Networks, in: G. Navarro-Arribas and V. Torra (Eds.), Advanced Research in Data Privacy, Springer International Publishing, 2015, pp. 303–324.
[22] S. Sandhya and K.S. Devi, Analysis of Bluetooth Threats and v4.0 Security Features, 2012 International Conference on Computing, Communication and Applications, ICCCA 2012, 2012, pp. 1–4.
[23] J. P. Dunning, Taming the blue beast: A Survey of Bluetooth Based Threats, IEEE Security and Privacy, 2010, vol. 8, no. 2, pp. 20–27.
[24] N. Vidgren, K. Haataja, J. L. Patiño-Andres, J. J. Ramírez-Sanchis, and P. Toivanen, Security Threats in ZigBee-enabled Systems: Vulnerability Evaluation, Practical Experiments, Countermeasures, and Lessons Learned, Proceedings of the Annual Hawaii International Conference on System Sciences, 2013, pp. 5132–5138.

[25] P. Pongle and C. Gurunath, A Survey : Attacks on RPL and 6LoWPAN in IoT, International Conference on Pervasive Computing (ICPC), 2015, pp. 1–6.
[26] K. Zhao and L. Ge, A Survey on the Internet of Things Security, Proceedings - 9th International Conference on Computational Intelligence and Security, CIS 2013, 2013, pp. 663–667.
[27] V. Davidovic, D. Ilijevic, V. Luk, and I. Pogarcic, Private Cloud Computing and Delegation of Control, 25th DAAAM International Symposium on Intelligent Manufacturing and Automation, DAAAM 2014, 2015, pp. 196–205.
[28] R. V. Rao and K. Selvamani, Data Security Challenges and Its Solutions in Cloud Computing, Procedia Computer Science, vol. 48, 2015, pp. 204–209.
[29] S. Husnjak, D. Peraković, I. Forenbacher, and M. Mumdziev, Telematics System in Usage Based Motor Insurance, 25th DAAAM International Symposium on Intelligent Manufacturing and Automation, DAAAM 2014, 2015, pp. 816–825.
[30] A. Knud and L. Lueth, "IoT market analysis : Sizing the opportunity IoT Analytics IoT market analysis : Sizing the opportunity," 2015. [Online]. Available: http://iot-analytics.com/iot-market-forecasts-overview/. [Accessed: 01-Jan-2015].
[31] Verizon, "The Internet of Things 2015," State of the Market, 2015. [Online]. Available: http://www.verizonenterprise.com/resources/reports/state-of-market-the-market-the-internet-of-things-2015.pdf. [Accessed: 03-Jan-2015].
[32] D. Peraković, M. Periša, and V. Remenar, Model of Guidance for Visually Impaired Persons in the Traffic Network," Transportation Research Part F, 2015, vol. 31, pp. 1–11.
[33] M. Periša, D. Peraković, and J. Vaculík, Adaptive technologies for the blind and visual impaired persons in the traffic network, Transport, 2015, vol. 30, no. 3, pp. 247–252.
[34] M. Periša, D. Peraković, and S. Šarić, Conceptual Model of Providing Traffic Navigation Services to Visually Impaired Persons, Promet- Traffic&Transportation, 2014, vol. 26, no. 3, pp. 209–218.