Avrupa Bilim ve Teknoloji Dergisi
Sayı 15, S. 36-42, Mart 2019
© Telif hakkı EJOSAT'a aittir
Araştırma Makalesi

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
No 15, pp. 36-42, March 2019
Copyright © 2019 EJOSAT
Research Article

A Survey on Security Threats and Solutions in the Age of IoT

Cihan Atac[1*], Sedat Akleylek[2]

[1] Ondokuz Mayis University, Department of Intelligent Systems Engineering, Samsun/Turkey (ORCID: 0000-0001-7385-4902)
[2] Ondokuz Mayis University, Department of Computer Engineering, Samsun/Turkey (ORCID: 0000-0001-7005-6489)

(First received 9 December 2018 and in final form 17 February 2019)

(**DOI:** 10.31590/ejosat.494066)

REFERENCE: Atac, C., & Akleylek, S. (2019). A Survey on Security Threats and Solutions in the Age of IoT. *European Journal of Science and Technology*, (15), 36-42.

Abstract

Internet of Things (IoT) is rapidly developing and glamorous technology in which machines and devices are connected and interacted with each other via Internet anywhere anytime. This technology, which brings advantages, facilities and efficiency in many areas from city management to smart buildings, from health-care to industry, from energy to agriculture, etc. has also brought numerous challenges in terms of security. IoT is vulnerable to various types of attacks, malfunctions and misuses due to these challenges reasoning such as resource limitations, heterogeneity, lack of standardization, mobility, architecture. In this paper, we present the state of art for cyber security issues in IoT. We provide a comparison for IoT security in different perspectives including threats, vulnerabilities and some countermeasures. We give some recommendations on the precautions and countermeasures for cyber security issues in IoT.

Keywords: cyber security, IoT security, threats, vulnerabilities.

IoT Çağında Güvenlik Tehditleri ve Çözümleri Üzerine Bir Araştırma

Öz

Nesnelerin İnterneti (IoT) makine ve cihazların her yerde ve her zaman internet üzerinden birbirleriyle bağlantılı ve etkileşimli olduğu, hızla gelişmekte olan göz alıcı bir teknolojidir. Şehir yönetiminden akıllı binalara, sağlık sektöründen sanayiye, enerjiden tarıma vb. birçok alanda avantajlar, kolaylıklar ve verimlilik sağlayan bu teknoloji, güvenlik açısından da birçok zorluğu beraberinde getirmiştir. IoT, kaynak kısıtlamaları, çeşitlilik, standardizasyon eksikliği, mobilite, mimari vb. nedenlerden kaynaklanan zorluklardan dolayı çeşitli saldırılara, arızalara ve kötüye kullanıma açıktır. Bu makalede, IoT siber güvenlik sorunları açısından en son ve en gelişmiş fikirleri sunuyoruz. IoT güvenliği açısından tehditleri, güvenlik açıkları ve önlemleri içeren bir karşılaştırma sağlıyoruz. Birçok siber güvenlik sorunu için tedbirler ve önlemler konusunda bazı öneriler veriyoruz.

Anahtar Kelimeler: siber güvenlik, IoT güvenliği, tehditler, güvenlik açıkları.

[*] Corresponding Author: Ondokuz Mayis University, Department of Intelligent Systems Engineering, Samsun/Turkey, ORCID: 0000-0001-7385-4902, cihan.atac@gmail.com

1. Introduction

Internet of Things (IoT) that are currently in infancy and which are developing at a dizzying pace, are changing and shaping our daily lives. The IoT is integrated and connected physical objects or things via network that is embedded with software, electronics, sensors for gaining greater value and service by exchanging data with manufacturers, operators and some other connected devices without human intervention [1]. There are plenty of IoT applications in various areas such as healthcare, automation and industrial manufacturing, electricity, smart city, agriculture, logistics, vehicular technology, retail, security, business management etc. IoT also serves for social needs such as surgery monitoring, weather condition detection, animal identification [2]. By collecting and analyzing data coming from IoT devices, it is possible to increase the efficiency of the entire system [2].

When we examine the architectural structure of IoT we can divide it into 3 main parts [1]:

1. The ‘‘things’’ (objects): Sensors, RFID tags and readers, BLE devices,
2. The communication networks that connect them: Cloud internetwork, WLAN, WSNs,
3. Data transfers from and to objects by using computer systems: Big Data applications.

The number of devices that are expected to be connected to Internet according to Gartner by 2020 is 50 billion. And this number is rising to 500 billion by 2030, according to Cisco. By 2020, IoT technology will be in 95% of electronics for new product designs [3].

Along with this rising, large amount of devices integrated and connected to internet and enormous data associated with it, issues about the security are mounting up with increasing momentum. For example, when we look at the number of malware samples for IoT devices in KasperskyLab’s collection, we see that it increases from 3.219 in 2016 to 121.588 in 2018.

Security issues reasoning from some factors in IoT can be listed as follows:

- A great deal of various devices and objects are connected and interacted together in a complicated way [4].
- Variation in technologies and standards are defined as one of the significant challenges in the development of IoT applications, since standardization of IoT architecture and communication technologies are basis for the IoT development [5].
- Because of lack in power, storage capacity, bandwidth and microprocessor, security countermeasures like public key encryption algorithm and frequency leaping communication cannot be applied [6].
- Security threats like abuse of resources, user and root compromise, virus, social engineering, trojan, worm, denial of services [5].
- The scale of the processed data is too large [6].
- Smart devices grow in extremely dynamic surroundings, where changes in the network topology are made often. This makes the deployment of security solutions very challenging [7].
- The servers for IoT are organized with cloud computing, and cloud computing has risks such as data security and privacy, data integrity, management, bandwidth, and data transfer [8].
- The fact that the cyber security solutions are not embedded in systems with the ‘security by design’ approach can make the solution of problems difficult, expensive and even impossible [21].
- Human factor is the most important factor in IoT security.

In this study, we provide a brief survey on the cyber security issues in IoT. Our aim is to give the state of the art with a different perspective. This includes the layers of IoT. We also focus on future directions and recommendations for the cyber security issues in IoT.

The organization of this paper is as follows: In Section 2, IoT security requirements and studies in literature are summarized. In Section 3, details for IoT vulnerabilities, caused threats and related solutions are given. In Section 4, conclusion with future works is presented.

2. Security Requirements for IoT

In this section, security requirements like availability, confidentiality and integrity etc. are discussed and then various approaches proposed in the literature to categorize vulnerabilities of IoT are evaluated.

There are apparently competing, complicated security requirements to be deployed on a platform with probably restricted resources [9].

Most important security and privacy requirements with cryptographic point of view are summarized in Figure 1.

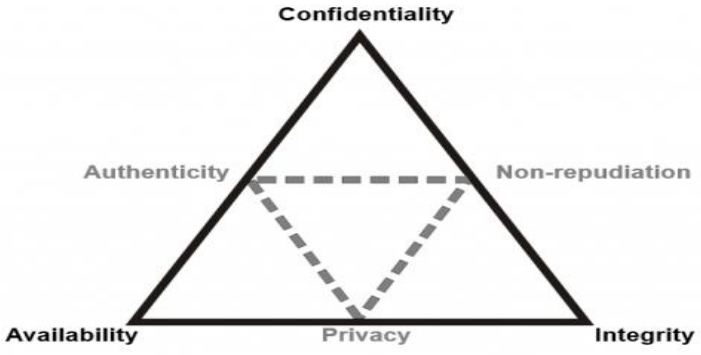


Figure 1. Security requirements

- *Availability*: It can be described as the system can continue to work even in the most critical conditions [7].
- *Authenticity*: Intrusion to the system or reaching delicate data by illegal users are not allowed [6].
- *Confidentiality*: Confidentiality provide that information is made obscure to unauthorized individuals, entities, and processes [7].
- *Integrity*: Integrity ensures that data has not been modified by a third party (accidentally or intentionally) [7].
- *Non-repudiation*: It assures that the sender of the message can not refuse having sent the message in the future [7].
- *Privacy*: It ensures that users' identities should not be identifiable nor observable from their actions and their movements in the system [7].

Many studies have been carried out to explain the security risks, weaknesses and challenges on IoT. Various approaches have been proposed in the literature to categorize the vulnerabilities of IoT.

The main focus of these works is the layers of IoT architecture centric security classification. On the basis of IoT architecture there are four layers. These are application layer, support (middle-ware) layer, network layer, perception layer and most of the studies discuss security threats and the solutions on these layers [6,22,23,24]. Apart from this, some studies approach security architecture model for IoT as three layered; endpoint and devices, network, data and applications and establish the security model on these [25,26]. Another approach classifies security concerns as human, process, data and object [4,27]. Separately, some studies look at major security challenges that exist in IoT environments by categorizing them as authentication, authorization and access control, privacy and secure architecture [10]. One common approach is classifying vulnerabilities and related solutions as insecure web interface, insufficient authentication/authorization, insecure network services, lack of transport encryption/integrity verification, privacy concerns, insecure cloud interface, insecure mobile interface, insufficient security configurability, insecure software/firmware, poor physical security [28].

3. Threats, Vulnerabilities And Related Solutions of IoT

In this section, new categorization including the vulnerabilities, threats of IoT and their solutions is presented. A detailed comparison is provided.

In the light of the previous studies, vulnerabilities of IoT and their solutions can be grouped as follows:

1. Insufficient authentication/authorisation mechanisms
2. Not using suitable cryptographic techniques
3. Cyber attacks
4. Privacy
5. Software/firmware related issues
6. Human factor

3.1. Insufficient Authentication/Authorisation Mechanisms

Authentication is the process of identifying users and devices in a network and confirming entry to authorized persons and reliable devices. Authentication is now the most popular method (60%) to grant access to the user at the application layer and also give access to the device in the IoT network [11].

Transport Layer Security (TLS) is broadly used for communication authentication and encryption. Specifically, for restricted devices, TLS offers TLS-PSK, which uses pre-shared keys, and TLS-DHE-RSA authentication method which uses RSA and Diffie-Hellman (DH) key exchange, which are public key and cryptographic protocols. Currently, there are three types of authentication protocols designed for IoT: asymmetric-cryptosystem based protocols, symmetric-cryptosystem based protocols, and hybrid protocols. Lately, there has been enormous demand for lightweight authentication and encryption [11].

It is about ineffective/poor mechanisms to authenticate or authorisation to IoT user interface whereby a user can gain higher levels of access [28].

Some countermeasures to protect the IoT system against the threats reasoning from related issue:

- ✓ Changing default passwords and usernames during initial setup [28].
- ✓ Assuring that web interface is not sensitive to XSS, SQLi or CSRF [28].
- ✓ Account lockout mechanism must step in after 3 -5 failed login attempts [28].
- ✓ Providing using the strong passwords [28].
- ✓ Making sure that password recovery mechanisms are trustworthy [28].
- ✓ Guarantee that the credentials are properly protected [28].
- ✓ Applying two factor authentication if reasonable [28].
- ✓ Providing that only required ports are exposed and available [28].
- ✓ Guarantee that user accounts cannot be enumerated using functionality such as password reset mechanisms [28].
- ✓ Underwriting network ports or services are not subject to internet via UPnP for example [28].

3.2. Not Using Suitable Cryptographic Techniques

The security of IoT is receiving great attention as the low power constraints and complexity features of many IoT devices are restricting the use of traditional cryptographic techniques [12].

Succeeding end to end security, the nodes are encrypted. However, due to the heterogeneity of the IoT systems, some nodes might be able to embed general purpose microprocessors. Nevertheless, low resources and constrained devices can only embed application-specific systems. Hence, traditional cryptographic primitives are not suitable for low-resource smart devices due to their low computation power, limited battery life, small size, small memory, and limited power supply. So, lightweight cryptography may be an efficient encryption for these devices [11].

Since the target for IoT encryption is to arrive efficient end to end communication with low power consumption, symmetric and asymmetric lightweight algorithms for IoT are designed to meet the requirements [11].

Some important countermeasures that should be taken are given below about the issue:

- ✓ Use of other industry-standard encryption techniques to protect data during migration if SSL/TLS is not available [6,28].
- ✓ Make sure that only the accepted encryption standards are used and that special encryption protocols are avoided [28].
- ✓ Securely encrypting the collected data [6,28].
- ✓ Guarantee IPsec (Internet Protocol Security) [6].

3.3. Cyber Attacks

IoT continues to grow as a primary target for cybercriminals to take advantage of, in step with a replacement threat report from security firm Symantec. The quantity of IoT attacks inflated from regarding 6,000 in 2016 to 50,000 in 2017 - a 600% rise in exactly one year, the report found [13].

- *DoS*: A denial-of-service (DoS) is any variety of attack wherever the attackers try and stop legitimate users from accessing the service by flooding servers, systems or networks with traffic in order to overwhelm the victim's resources [14].
- *DDoS*: A distributed denial-of-service (DDoS) attack is a malicious initiative to break normal traffic of a purposed server, service or network by crushing the target or its ambient infrastructure with a flood of internet traffic [15]. From many perspectives, it resembles a DoS attack, but the results are very different. In place of one computer and one internet connection the DDoS attack employs many computers and many connections. The computers behind such an attack are often deployed around the whole world and will be part of botnet [29].
- *Malicious code*: Malicious code is the sort of destructive computer code or web script intended to create system vulnerabilities causing to back doors, security breaches, information and data theft, and other possible damages to files and computing systems [16].
- *Eavesdropping*: Eavesdropping is defined as electronic attack wherever digital communications are intercepted by a private whom they're not supposed. This is wiped out 2 main ways: Directly taking note of digital or analogue speech communication or the interception or sniffing of information regarding any kind of communication [17].
  - *Smurf*: A Smurf attack could be a variety of a distributed denial of service (DDoS) attack that renders pc networks inoperable. The Smurf program accomplishes this by exploiting vulnerabilities of the Internet Protocol (IP) and Internet Control Message Protocols (ICMP) [18].
  - *Spoofing*: Spoofing, in general, could be a dishonourable or malicious observe within which communication is distributed from an unknown supply disguised as a supply best-known to the receiver. Spoofing is most current in communication mechanisms that lack a high level of security [19].

Leading solutions to these threats are presented below:

- ✓ Using effective antivirus and firewall [6,8].
- ✓ Utilize data encryption [6,8,28].
- ✓ Running powerful authentication, authorization and access control mechanisms [6,8,28].
- ✓ Operating well IPS (Intrusion Prevention System) and IDS (Intrusion Detection System) [6,8].

3.4. Privacy

Privacy represents the stress evoked by the interaction between person and technological scheme. Information being protected is essentially associated with persons, therefore their privacy may be an obligatory objective of the IoT. Also, misuse of technology may be an explanation for privacy violation [20]. Privacy issues are generated by the gathering of non-public information additionally to the shortage of correct protection of that information [28].

- ✓ Gathering only data that is critical to the functionality of device [28].
- ✓ Securely encrypting the collected data [28].
- ✓ Correct protection of the device and all its components [28].
- ✓ Guarantee that only authorized persons have access to personal information gathered [28].
- ✓ Assure that storage limits are set for the gathered data [28].

3.5. Software/Firmware Related Issues

Software/firmware updates for devices can be insecure when the updated files themselves and the network connection they are delivered on are not protected [28]. Important threats can be classified as follows:

- Problems on update issues
- Firmware contains sensitive information [28].

Solutions to these issues are pointed out as follows:

- ✓ Providing the ability to update the device [28].
- ✓ Encrypting the update file using accepted encryption methods and transmitting it via an encrypted connection [28].
- ✓ Guarantee that firmware include no susceptible information [28].
- ✓ Providing that the update file is transmitted over an encrypted connection [28].
- ✓ Make sure that the update server is secure [28].
- ✓ Guarantee that firmware includes no susceptible data [28].

3.6. Human Factor

IoT has diverse and extensive structure, so security limitations and threats are more probable. Because of this, large numbers of persons with different security background levels according to respective characters are influenced from the issue. According to respective roles, consumers, end users, and service or technology providers are involved in IoT context [4].

The user information of the IOT device or application can be captured by e-mail fraud, phishing, spam or session hijack methods and used for malicious purposes.

For example, smart tv may be captured by malicious persons and its sources can be used for bad purposes. When detecting spam and phishing e-mail cases of 75 million using smart tv or refrigerator connected to the Internet, it is found that zombie home appliances were real like zombie PC [30].

Also in military, using replay or session hijacking attack techniques, incorrect information may be inserted on target device. By doing so, it is possible to delay the friendly operations or cause the confusion [30].

There are head weaknesses and threats reasoning from or taking aim to people. These are:

- *Not acting over a security management rules* [20].
- *Social Engineering*: It is type of attack that is performed by deceiving people, in order to get information about the person in the target system [8].
- *E-mail fraud*: It is a type of attack that is performed by showing the fake e-mail address as reliable [8].
- *Web forgery*: It is type of attack that is performed using the fake of a trusted website [8].
- *Session hijack*: It is type of attack performed between the client and the server to capture the user's session [8].
- *Phishing*: It is type of attack to capture personal information by e-mail [8].
- *Spam*: It is attack sort that the messages come to e-mails of the target system for any purpose [8].

The countermeasures to be taken against these threats and weaknesses are listed as follows:

- ✓ Examine and control security practices and rules to develop effective security policy documentation [20].
- ✓ Organizing awareness raising education programs and activities.
- ✓ Using effective antivirus and firewall [6,8].
- ✓ Use of single-use password and encryption algorithm [6,28].
- ✓ Secure protocols usage [8].

IoT-related vulnerabilities, threats and the countermeasures are summarized in Table 1. In this table, the IoT vulnerabilities are taken over 6 groups, the main threats that these weaknesses can be caused and the countermeasures to be taken against these threats are presented.

4. Conclusion and Recommendations

IoT, which develops at a fast pace and connects many and various objects to internet by its nature, brings many security challenges along with the opportunities it offers In this study, after giving brief information about the IoT and its structure, the reasons of the challenges of IoT cyber security were emphasized, then security requirements to be provided were mentioned and vulnerabilities were grouped with a different perspective and the related solutions were discussed. By using IoT components by attackers, it has been seen that the main elements of information security can be targeted and serious threats can be created on a personal, institutional or national basis. It has been understood that considerable effort is needed to minimize vulnerabilities and threats mentioned in the study.

In order to improve IoT security, there are several countermeasures to enhance it. Systems should be structured according to security policies and standards from the design stage. IoT endpoint devices are often the weakest link in the systems of security. Therefore, to ensure safety of these devices, it is necessary to detect all abnormalities by monitoring all Internet traffic instead of restricting Internet, and in this case, warning and blocking mechanisms should be activated. Optimized asymmetric cryptography solutions can solve problems such as complexity and scalability. With regard to privacy, IoT data can be

collected and analysed, and then potential threats can be identified and resolved. Efficient work on new generation wireless network technologies and protocol design can lead to increased security.

Acknowledgments

This research is partially supported by OMÜ under grant no. PYO.MUH. 1906. 17.003.

The authors would like to express their gratitude to the anonymous reviewers for their invaluable suggestions in putting the present study into its final form.

Table 1. IoT vulnerabilities, threats and their solutions

Vulnerabilities	Threats	Solutions
Insufficient authentication /authorization mechanisms	▪ Gaining unauthorized or high lev access to the data or device ▪ SQL Injection ▪ XSS or CSRF	✓ Changing default passwords and usernames during initial setup [28]. ✓ Assuring that web interface is not sensitive to XSS, SQLi or CSRF [28]. ✓ Providing using strong passwords [28]. ✓ Guarantee that credentials are properly protected [28]. ✓ Applying two factor authentication if reasonable [28]. ✓ Providing that only required ports are exposed and available [28].
Not using suitable cryptographic techniques	▪ Sniffing or capturing data or compromising the device by an intruder ▪ Man in the middle ▪ Sybil ▪ Replay attack	✓ Use of other industry-standard encryption techniques to protect data during migration if SSL or TLS is not available [6,28]. ✓ Make sure that only accepted encryption standards are used and that special encryption protocols are avoided [28]. ✓ Securely encrypting the collected data [6,28]. ✓ Guarantee IPsec (Internet Protocol Security) [6].
Cyber attacks	▪ Dos ▪ DDos ▪ Malicious code ▪ Eavesdropping ▪ Smurf ▪ Spoofing	✓ Using effective antivirus and firewall [6,8]. ✓ Utilize data encryption [6,8,28]. ✓ Running powerful authentication, authorization and access control mechanisms [6,8,28]. ✓ Operating well IPS (Intrusion Prevention System) and IDS (Intrusion Detection System) [6,8].
Privacy	▪ Collection of unnecessary personnel information ▪ Lack of proper protection of data	✓ Gathering only data that is critical to the functionality of the device [28]. ✓ Securely encrypting the collected data [28]. ✓ Correct protection of the device and all its components [28].
Software / firmware related issues	▪ Problems on update issues ▪ Firmware contains sensitive informatio	✓ Providing ability to update the device [28]. ✓ Encrypting the update file using accepted encryption methods and transmitting it via an encrypted connection [28]. ✓ Guarantee that firmware include no susceptible information [28].
Human factor	▪ Not acting over a security management rules ▪ Social Engineering ▪ E-mail fraud ▪ Web forgery ▪ Session hijack ▪ Phishing ▪ Spam	✓ Examine and control security practices and rules to develop effective security policy documentation [20]. ✓ Organizing awareness raising education programs and activities ✓ Using effective antivirus and firewall [6,8]. ✓ Use of single-use password and encryption algorithm [6,28]. ✓ Secure protocols usage [8].

References

[1] Stergiou, C., Psannis, K.E., Kim, B.,Gupta, B., (2018). Secure integration of IoT and Cloud Computing. *Future Generation Computer Systems, 78*, 964–975.

[2] Khan, M.A., Salah, K., (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems, 82*, 395–411.

[3]Panetta, K. (03.11.2017). *Gartner Top Strategic Predictions for 2018 and Beyond*. Retrieved from https://www.gartner.com/smarterwithgartner/gartner-top-strategic-predictions-for-2018-and-beyond/), on (02.11.2018).

[4] Sfar, A.R., Natalizio E., Challal, Y., Chtourou, Z., (2018). A roadmap for security challenges in the Internet of Things. *Digital Communications and Networks, 4*, 118–137.

[5] ˇColakovi ´c, A., Hadžiali ´c, M., (2018). Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues. *Computer Networks, 144*, 17–39.

[6] Jaychand, Behar N., (2017). A Survey on IoT Security Threats and Solutions. *International Journal of Innovative Research in Computer and Communication Engineering, Vol. 5, Issue 3*.

[7] Kouicem, D.E., Bouabdallah, A., Lakhlef, H., (2018). Internet of things security: A top-down survey. *Computer Networks, 141*, 199–221.

[8] Ülker, M., Canbay, Y. Sağıroğlu, Ş., (2017). Examination of Internet of Things in Terms of Personal, Enterprise and National Information Security. *Journal of Turkey Informatics Foundation of Computer Science and Engineering, 10.*

[9] Xu, L.D., Li, S., (2017). *Securing the Internet of Things*. Syngress.

[10] Conti, M., Dehghantanha, A., Franke, K., Watson, S., (2018). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems, 78* 544–546.

[11] Noor, M.M., Hassan,W.H., (2018). Current research on Internet of Things (IoT) security: A survey. *Computer Networks.*

[12] Zhang, J., Duong, T., Woods, R., Marshall, A., (2017). Securing Wireless Communications of the Internet of Things from the Physical Layer, An Overview. *Entropy, 19*, 420.

[13]Rayome, A.D. (21.03.2018). *As IoT attacks increase 600% in one year, businesses need to up their security*. Retrieved from (https://www.techrepublic.com/article/as-iot-attacks-increase-600-in-one-year-businesses-need-to-up-their-security/), on (26.09.2018)

[14] Denial-of-Service Attack (DoS). Retrieved from (https://www.techopedia.com/definition/24841/denial-of-service-attack-dos), on (02.11.2018)[15] What is a DDoS Attack . Retrieved from (https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/), on (03.11.2018).

[16] What is Malicious Code?. Retrieved from (https://www.kaspersky.com/resource-center/definitions/malicious-code), on (03.11.2018).

[17] Eavesdropping. Retrieved from (https://www.techopedia.com/definition/13612/eavesdropping), on (03.11.2018).

[18] What is a Smurf Attack?. Retrieved from (https://usa.kaspersky.com/resource-center/definitions/smurf-attack), on (04.11.2018).

[19] Spoofing. Retrieved from (https://www.techopedia.com/definition/5398/spoofing), on (07.11.2018)

[20] Riahi, A., Natalizio, E., (2014). A systemic and cognitive approach for IoT security. International Conference on Computing, Networking and Communications.

[21] Cha, S., Baek, S., Kang, S., Kim, S., (2018). Security Evaluation Framework for Military IoT Devices. Security and Communication Networks, Volume 2018, Article ID 6135845,12 Pages.

[22] Cvitić, I., Vujić, M., Husnjak, S., (October 2015). Classification of Security Risks in the IoT Environment. 26th Daaam International Symposium On Intelligent Manufacturing And Automation.

[23] Kumar, S.A., Vealey, T., Srivastava, H., (2016). Security in Internet of Things: Challenges, Solutions and Future Directions. 49th Hawaii International Conference on System Sciences.

[24] Alabaa, F.A., Othmana, M., Hashema, I.A.T., Alotaibib, F., (2017). Internet of Things security: A survey, Journal of Network and Computer Applications, 88, 10-28.

[25] How to Overcome IoT Security Concerns, (May,2017). A report in the IoT. InfoBrief Series, Sponsored by Bell.

[26] Sedrati, A., Mezrioui, A., (2018). A Survey of Security Challenges in Internet of Things. Advances in Science, Technology and Engineering Systems Journal Vol. 3, No. 1, 274-280.

[27] Gündüz, M.Z., Daş, R., (2018). Internet of things (IoT): Evolution, components and application fields. Pamukkale University Journal of Engineering Sciences, 24(2), 327-335.

[28] Internet of Things Top Ten. Retrieved from https://www.owasp.org/images/7/71/Internet_of_Things_Top_Ten_2014-OWASP.pdf), on (25.09.2018)