Scientific Research Publishing

Journal of Computer and Communications, 2017, 5, 121-136
http://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

A Review of Security Concerns in Internet of Things

Engin Leloglu

R&D Department, Vestel Electronic Inc., Manisa, Turkey
Email: engin.leloglu@vestel.com.tr

How to cite this paper: Leloglu, E. (2017) A Review of Security Concerns in Internet of Things. *Journal of Computer and Communications*, **5**, 121-136.
http://dx.doi.org/10.4236/jcc.2017.51010

Received: December 13, 2016
Accepted: January 19, 2017
Published: January 22, 2017

Abstract

The Internet of Things (IoT) represents a technologically optimistic future where objects will be connected to the internet and make intelligent collaborations with other objects anywhere, anytime. Although it makes appreciable development, there are still uncertainties about security concepts of its usage that is usually considered as a major concern in the design of IoT architectures. This paper presents a general survey of all the security issues in IoT along with an analysis of IoT architectures. The study defines security requirements and challenges that are common in IoT implementations and discusses security threats and related solutions on each layer of IoT architecture to make this technology secure and more widespread accordingly.

Keywords

Internet of Things, IoT, Security Requirements, Security Challenges, Security Threats, Security Solutions

1. Introduction

Although Internet of Things (IoT) is a well-known term and a rising trend in IT arena, there has been no agreed definition by the world community of users until now. In fact, there are many different groups in industry and standardization organizations that formulate similar ideas but in different forms and based on different components or aspects of an IoT system.

The best definition for the Internet of Things would be defined by ITU-T Y.2060:

> "Global infrastructure for the society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies."

IoT is such a system that supplies connectivity and interactive communication

for anything. Even though "being connected" is usually used in term of electronic devices in our daily life, physical objects that have hardware such as sensors or actuators, connect to the Internet with unique addresses. Data of physical object are transmitted continuously through wired/wireless networks to platforms where it will be interpreted. Physical objects are capable of understanding complexity of the environment and reacting due to their feature of sense and communication. The revolutionary advance in this case is that physical objects begin to be deployed and adopted widely. In addition, most of them begin to work properly without human intervention [1].

In future, every object in our daily life will be connected to Internet. Mobile phones will be used as the center point or the remote control for all objects in the physical world commonly called as IoT [2]. According to Gartner [3], it is expected that the number of Internet-connected devices will increase from around 25 billion to 50 billion by 2020. Prevalence of such a big network induces new security risks that can allow attackers to steal even more personal information about the users or the organizations that are connected to such an IoT system.

Emphasizing security issues surrounding IoT is the main goal of this paper. Security is an important concern for IoT technology because of following reasons [4]:

- IoT is accepted as an extended version of some different technologies such as Wireless Sensor Networks, Mobile Broadband and 2G/3G Communications Networks which are already under threat because of various security flaws.
- Every device is connected to Internet in IoT technologies and Internet is an unsecured environment naturally. There are many evil-minded people who are on the lookout for various system breaches and remote code executions.
- Objects in IoT communicate with each other; hence, there is a possibility that privacy and security can be hindered.

This study presents a general survey of all the security issues in IoT along with an analysis of IoT architectures. The paper describes security requirements and challenges that are usually faced in IoT implementations and mentions security threats and related solutions on each layer of IoT architecture to make this technology secure and more widespread.

The paper is organized as follows. In Section 2, IoT scope and recommended architecture are described. Section 3 studies security requirements and challenges for IoT implementations. In Section 4, security threats plaguing the Internet of Things are surveyed in such a way that all these threats are categorized based on layers of IoT architecture. Section 5 discusses security solutions and research directions on each layer and finally Section 6 concludes this study.

2. IoT Scope and Architecture

IoT purposes to enable things to be connected anyplace and anytime using any service/network [5]. Having this purpose of IoT in mind, it is stated that a correct and easy implementation of an IoT system mainly depends on identifying

the right principles regarding the proper discovery, identification, configuration and manipulation of interconnected devices and sensors [6].

In the study of Uma Mahesh *et al.* [7], a classification is proposed that helps in defining the various elements of IoT from a higher level perspective;

a) Hardware: Sensors, central units and built-in communication hardware are included in this level. Since a sensor has limited hardware, it is usually utilized in sensor networks that multiple sensors are linked together. A central unit that is a source of centralized services in IoTs, has a capable of storing, processing, and delivering data to users.

b) Middleware: It consists of storage and calculation tools for data analytics. Cloud computing is given as an example in this section.

Cloud computing is the integrity of several traditional technologies such as hardware virtualization, service-oriented architecture, load-balancing, distributed computing, grid computing, utility computing and autonomic computing. It can be considered as a natural step forward from the grid-utility model [8]. This style of computing relies on sharing of resources are provided as a service over the Internet to achieve coherence and economy of scale.

c) Presentation: There are visualization and interpretation tools in presentation level. These tools are designed for various applications and can be accessed from any platform.

From the network point of view, the opportunity of accessing information through tagged object by browsing on Internet primarily inspired the idea of IoT. Bringing objects into the digital world and identifying them by using their Internet addresses are supplied with different tagging technologies such as RFID, NFC and QR Codes [9]. RFID, intelligence embedded technology, sensor technology and nano-technology are pioneer technologies for the development of IoT. Radio frequency identification (RFID) is the foundation and networking core of the construction of IoT among them [10]. Kevin Ashton who was a pioneer of IoT underlines this issue in his article that RFID and the sensor technology strengthen traditional computers and gain them some significant features such as observation, identification and understanding the world of sensor data [11].

Wireless sensor network (WSN) is another type of data collection technology of the IoT that has some features to maintain the control over many nodes through wireless communication such as multi-hopping and self-organization. A WSN system contains a central unit that provides wireless connectivity back to the wired world and distributed nodes [12]. Each node is equipped with a sensor to detect physical phenomena such as light, heat, pressure, etc. [13]. Cooperative sensing, collecting and processing sensor information are purposes of this network model. The system can execute data collection and quantification, processing fusion and transmission application [14].

According to Jian An *et al.* [15], the architecture of IoT should be an open architecture, using open protocols to support a variety of existing network applications. Likewise, it should additionally incorporate security, adaptability and se-

mantic representation middleware to promote data world integration with Internet. In consideration of these ideas and some related studies [1] [16] [17] [18] [19] [20], the architecture in **Figure 1** is proposed to guide theoretical research.

1) Perception Layer: The sensor technology, intelligence embedded technology, nano technology and tagging technology are located in this layer. Main purpose of the layer is the identification of unique objects and the collection of information from the physical world with the help of its sensors [21].

2) Network Layer: It contains WSN, optical fiber communication networks, broad television networks, 2G/3G communications networks, fixed telephone networks and closed IP data networks for each carrier. Transfer of collected information from sensors, devices, etc., to an information processing system is under the responsibility of this layer.

3) Support Layer: The layer involves information processing systems which takes information in one form and processes (transforms) it into another form. This processed data is stored in a database and will be available when there is a demand. This layer works very closely with applications. Therefore, researchers prefer to place it in application layer [22].

4) Application Layer: In this layer, there are practical and useful applications which are developed based on user requirements or industry specifications such as smart traffic, precise agriculture, smart home, mining monitor, etc.

3. Security of IoT

3.1. Existing Requirements and Challenges of Security

Hui Suo *et al.* [18] refer that IoT extends the term of 'internet' through corresponding technologies such as traditional Internet, mobile networks, sensor networks and so on. Every "thing" is connected to this "Internet" and these "things" communicates with each other. According to Rolf H. Weber [23], these kinds of systems imply great potential for flexibility and scalability, but they have the risk of having security problems too. There are many issues about its wide adoption and without offering relevant solutions for the newly posed threats; it looks like it cannot be a practically applicable technology in close future.

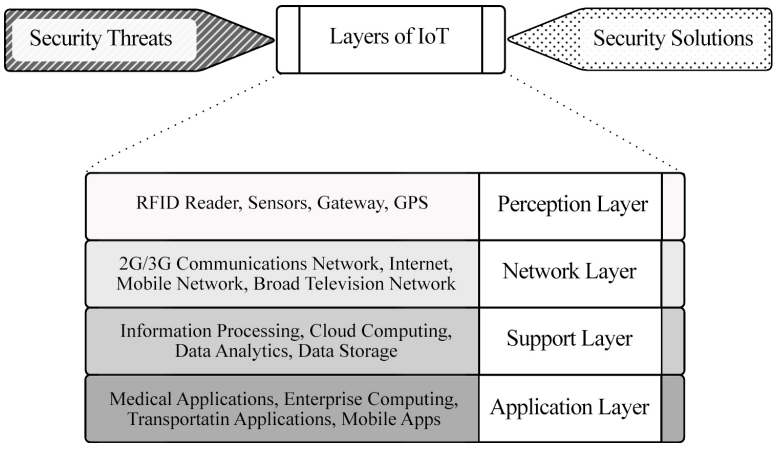

Figure 1. IoT Architecture.

Security requirements are examined in studies [21] [16] [18] [24] [19] [25] [26] in different dimensions. The requirements addressed in many studies can be summarized under five headings in Table 1.

In order to fulfill these requirements in Table 1, there are several challenges [21] [6] [16] [17] [27] [19] [26] [28] that must be handled in Table 2.

3.2. Existing Security Threats in IoT Systems

In this section, existing threats in IoT systems are examined in four categories based on IoT architecture which have been addressed in Section 2. The examination is summarized in Figure 2.

Table 1. Security requirements.

Authenticity:	Only legal users should be allowed to access the system or sensitive information [16].
Authorization:	The privileges of device components and applications should be limited as so they are able to access only the resources they need to do their addressed tasks [25].
Confidentiality:	Information transmission between the nodes should be protected from intruders [18].
Integrity:	Related information should not be tampered [19].
Availability and Continuity:	In order to avoid any potential operational failures and interruptions, availability and continuity in the provision of security services should be ensured [26].

Table 2. Security challenges.

Interoperability:	Relevant security solutions should not prevent the functionality of interconnected heterogeneous devices in IoT network system [27].
Resource constraints:	In IoT architecture, most of nodes lack of storage capacity, power and CPU. They generally use low-bandwidth communication channels. Hence, it is unable to apply some security techniques such as frequency hopping communication and public key encryption algorithm. Setup of security system is very difficult under these circumstances [6].
Data volumes:	Although some IoT applications use brief and infrequent communication channels, there are considerable number of IoT system such as sensor-based, logistics and large scale system that have potentials to entail huge volume of data on central network or servers [28].
Privacy protection:	Since a great number of RFID systems are short of suitable authentication mechanism, anyone can tracks tags and find the identity of the objects carrying them. Intruders can not only read the data, but can also modify or even delete data as well [21].
Scalability:	The IoT network consists of a large number of nodes. The proposed security mechanism on IoT should be scalable [19].
Autonomic control:	Traditional computers need users to configure and adapt them to different application domains and different communication environments. However, objects in IoT network should establish connections spontaneously, and organize/configure themselves for adapting to the platform they are operating in. This kind of control also involves some techniques and mechanisms such as self-configuring, self-optimizing, self-management, self-healing and self-protecting [27].

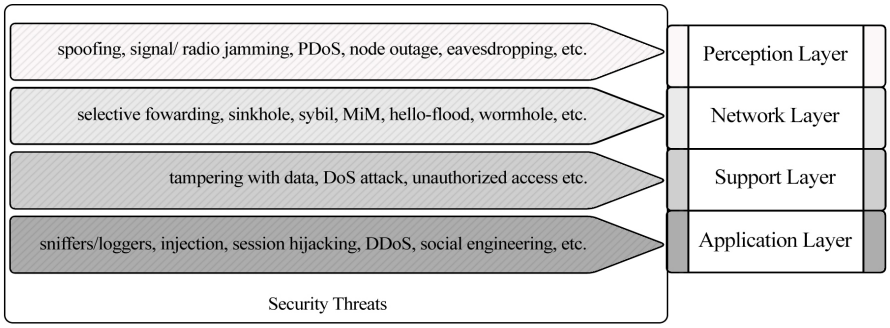

Figure 2. Threats on layers of IoT.

3.2.1. Threats of Perception Layer

Sensor and intelligence embedded technologies including RFID readers, sensors or GPS are under threat because of various security flaws. Main threats are discussed below:

Spoofing: It is initiated with a fake broadcast message sent to sensor network by the attackers. It makes it to assume its originality falsely which makes it appearing from the original source [29]. It is quite often that this scenario is results in the attacker obtaining full access to the system making it vulnerable.

Signal/Radio Jamming: It is a type of DoS attack that it occupies the communication channel between the nodes and hinders them from communicating with each other [30].

Device-tampering/Node-capturing: The attacker captures the sensor node physically replaces the node with their malicious node. This type of attack usually results in the attacker gaining total control over the captured node and harms the network [31].

Path-based DoS Attack (PDoS): In this type of DoS attack, the attacker overpowers sensor nodes a long distance away by flooding a multihop end-to-end communication path with either replayed packets or injected spurious packets [32]. Diminished system availability and exhaustion in batteries of nodes are impacts of this physical attack.

Node Outage: The attack is applied logically or physically to the network and it stops the functionality of network components. Node services such as reading, collecting and initiating operations are stopped because of this attack [31].

Eavesdropping: Wireless characteristics of RFID system make it possible that attacker sniffs out the confidential information such as password or any other data flowing from tag-to-reader or reader-to-tag making the system vulnerable [21] [33].

Various kinds of perception layer attacks are listed below with related risks on security mechanisms of IoT in **Table 3**.

3.2.2. Threats of Network Layer

Network layer which is known as the next-generation network are exposed to many kinds of threats. Related threats that come from this layer are listed below:

Selective Forwarding: In such attacks, malicious nodes do not forward some messages and selectively drop them, ensuring that they cannot propagate later

Table 3. Attacks and related risks on security mechanisms of IoT.

Attacks	Risks
Spoofing	Authenticity, integrity and confidentiality.
Signal/Radio Jamming	Availability and integrity.
Device-tampering/Node-capturing	Availability, integrity, authenticity and confidentiality.
Path-based DoSAttack	Availability and authenticity.
Node Outage	Availability and authenticity.
Eavesdropping	Confidentiality.

on. The attacker who is responsible for suppression or modification of packets originating from a select few nodes can sometimes forward the remaining traffic not to reveal her wrongdoing. There are different types of selective forwarding attacks. In one type, the malicious node can selectively drop the packets coming from a particular node or a group of nodes. This situation poses a risk of DoS attack for that node or a group of nodes. Another type of selective forwarding attack is called Neglect and Greed. In this type of attack, the subverted node arbitrarily skips routing some messages [34].

Sybil Attack: It is clarified as a malicious device illegitimately taking on multiple identities [35]. Sybil attack [36], an attacker can "be in more than one place at once" as a single malicious node. It presents multiple identities to other nodes in the network reducing the effectiveness of fault tolerant schemes.

Sinkhole Attack (*Blackhole*): The sink hole is defined in [37] by intense resource contention among neighboring nodes of the malicious node for the limited bandwidth and channel access. It results in congestion and can accelerate the energy consumption of the nodes involved. With sink holes forming in a sensor network, it is vulnerable to several other types of denial of service attacks [38] [37] [39].

Wormhole: This form of DoS attack induces relocation of bits of data from its original position in the network. This relocation of data packet is carried out through tunneling of bits of data over a link of low latency [39].

Man-in-the-Middle Attack: This attack is described as a form of eavesdropping in which the unauthorized party can monitor or control all the private communications between the two parties hideously. The unauthorized party can even fake the identity of the victim and communicate normally to gain more information [21].

Hello-flood Attack: High traffic in channels is the main disrupting effect of this attack which congests the channel with an unusually high number of useless messages. Basically, a single malicious node sends a useless message which is then replied by the attacker to create a high traffic [30].

Acknowledgement Flooding: Routing algorithms in sensor-based systems need acknowledgements from time to time. In this type of DoS attack, a malicious node sends false information to destined neighboring nodes by the help of these acknowledgements [30].

3.2.3. Threats of Support Layer

Target of threats in support layer are mainly data storage technologies. These threats are discussed below:

Tampering with Data: The attack appears when a person from the inside tampers the data for personal benefits or commercial benefits of any 3rd party companies. The data can be extracted and modified easily on purpose from the inside [17].

DoS Attack: Similar effects of DoS attacks that are discussed in previous layers are seen in this layer, too; e.g. it shuts down the system which results in unavailability of the services.

Unauthorized Access: The attacker can easily infiltrate into the system and damage the system by preventing the access to the related services of IoT or deleting sensitive data. Hence, an unauthorized access can be fatal for the system [21].

3.2.4. Threats of Application Layer

The personalized services based on the needs of the users are included in the application layer; e.g. the interface that user can control devices in IoT [4]. Threats in this layer mainly target these services as mentioned below:

Sniffer/Loggers: Attackers can introduce sniffer/logger programs into the system that take important information from the network traffic. The main goal of the sniffer is to steal passwords, files (FTP files, E-mail files), and E-mail text. Many protocols are prone to sniffing [40].

Injection: Attackers may enter code directly into the application that is executed on the server. This is a very common attack, easy to exploit, and can cause some bad results such as data loss, data corruption and lack of accountability [41].

Session Hijacking: This attack reveals personal identities by exploiting security flaws in authentication and session management. This type of attack is very common and effects of attack are really important. With the identity of someone else, attacker can do anything the real user can do [41].

DDoS (*Distributed Denial of Service*): Its working principle is the same as the traditional Denial of Service attack. However, it is executed by multiple attackers at the same time [21] [30] [41].

Social Engineering: A serious threat for application layer where attackers can obtain information from users via chats, knowing each other etc. [4].

3.3. Recommended Solutions and Research Directions with Respect to Security in IoT

Recommended solutions and research directions with respect to security in IoT are examined in three categories: security of perception layer, security of network layer and security of support and application layers. The examination is summarized in **Figure 3**.

3.3.1. Security of Perception Layer

Taking security measures for the perception layer dates back times before IoT.

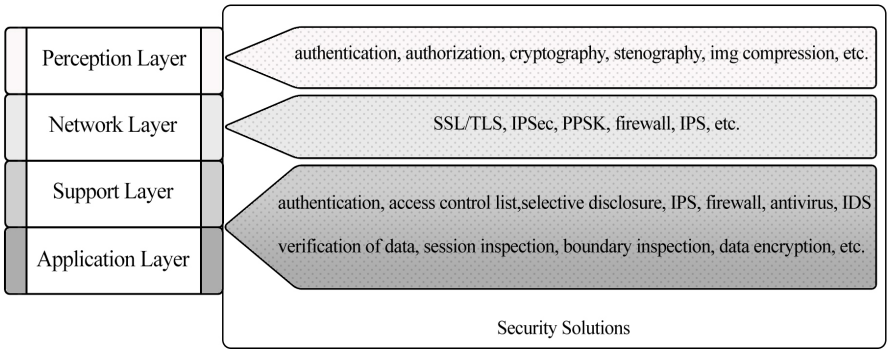

Figure 3. Security solutions on layers of IoT.

Table 4. Cryptograhic algorithms.

Type	Algorithm	Purpose
Symmetric Encryption	Advanced encryption standard (AES)	Confidentiality
Asymmetric Encryption	Rivestshamir Adelman (RSA)/Elliptic curve cryptography (ECC)	Digital Signatures, Key Transport
Asymmetric Key Agreement	Diffie-hellman (DH)	Key Agreement
Hashing	SHA-1/SHA-256	Integrality

Equipments such as RFID readers, sensors, gateways, GPS and other devices require to be secured efficiently. OWASP has identified poor physical security in the top 10 IoT vulnerabilities [42]. The first step is to ensure that only authorized people can have access to sensitive data produced by physical objects, that's why a physical identity and access management policy need to be defined [43]. Authentication and authorization requirements from IoT are satisfied in this similar fashion.

Data collection is an important issue for this layer. In [44], this issue is examined in two separate headings. In one heading which is presented as multimedia data collection, there are some recommended security techniques such as multimedia compression, stenography, water marking, encryption, time session and intellectual property. The second heading is image data collection, to use security in images as image compression, and CRC.

Cryptographic processing is one of the main tasks in security mechanisms for sensor data on IoT. These operations that are often used in order to guarantee privacy of data include encryption and decryption, key and hash generation, and sign and verify hashes. **Table 4** gives some frequently used cryptographic algorithms and their use purposes in Internet security protocols based on studies [18] and [45].

Wander *et al.* [46] compare two asymmetric algorithms in **Table 4**, RSA and Elliptic Curve Cryptography (ECC) [47], on sensor nodes and prove that ECC is more efficient than RSA, and asymmetric cryptography is applicable for resource-constrained hardware. Hence, researchers focus on reducing complexity of asymmetric cryptographic algorithms and key distribution protocols. Wood *et al.* [48] and Hu *et al.* [49] present hardware cryptographic solutions for smart

objects in their study. Key distribution mechanism of Liu *et al.* [50] and Chung *et al.* [51] are demonstrated in order to use in lightweight communication channels in resource-constrained networks. These improvements make cryptographic mechanisms in the context of WSNs more applicable. However, unique customized solutions are created and still there has been no standardized way of implementing services [52].

Risk Assessment is a fundamental of IoT security which determines the extent of the potential threat and the risk associated with an IoT system. The output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process. A number of organizations have developed guidelines for conducting risk assessment such as the U.S. National Institute of Standards and Technology (NIST) [53] [54]; the International Standards Organization (ISO) and the International Electrotechnical Commission (IEC) [55].

3.3.2. Security of Network Layer

The security of network layer can be examined in two main sub-layers; wireless and wired. One of the initial actions in wireless security sub-layer is the development of protocols for authentication and key management [56]. For example; SSL/TLS is developed to encrypt the link in the transport layer, and IP security protocol (IPSec) is developed to keep the network layer secure. They can provide authenticity, confidentiality and integrity in the each layer [18]. Also, using PPSK (Private Pre-Shared Key) for each sensor or device connected to the network provides another security measure for IoT system. By providing different unique keys, the access domain for each type of device can be defined easily. Moreover, disabling guest and default passwords in network devices such as routers and gateways should be done immediately upon installing a new network device. This includes strong password policies, password management and periodic change of passwords [43].

The wired security sub-layer is concerned with devices, which communicate with other devices on the IoT system using wired channels. Common security techniques are applied in wired type networks are firewalls and Intrusion Prevention System (IPS). If the network has firewall or IPS, it can inspect network packets deeply that are destined towards the destination. However, existing IoT has no ability in terms of packet inspection and packet filtering. There is an ongoing research on this issue where security researchers try to design a low resource-hungry firewall for IoT to provide the ability of packet inspection [4].

All information about the security of network layer that is discussed above is summarized in **Table 5**.

3.3.3. Security of Support and Application Layers

Devipriya *et al.* [44] claims that this topic contains two sub-layers. In one sub-layer, there are local applications and related middleware functions which should be secured with various techniques. For example, intelligent transportation systems can use encryption techniques, while smart home/smart metering

Table 5. Security of Network Layer on IoT.

Sub-layers	Security Techniques	Purposes
Wireless	TLS/SSL	Authenticity, Confidentiality, Integrity
	IPSec	
	PPSK	
Wired	Firewall	
	IPS	

systems uses steganography techniques. The second sublayer corresponds to national applications and their security systems, ensuring that sent and received data are secure. Therefore, various security techniques are applied in these systems based on the scope of each system such as authentication, authorization, access control list, selective disclosure, intrusion detection, firewall, and antivirus.

According to Farooq *et al.* [21], authentication mechanism preventing the access of intruders is applied in support and application layer by integrated identity identifications. This identity security mechanism is exactly similar to that in the network layer. The difference is that these layers focus on authentications by some certain cooperating services which means users can even choose the associated information to be shared with the services.

Data security is another issue on these layers [57]. There are various precautions taken by security system on IoT such as:

- Safe programming and anti-virus software testing against malicious code injections and service loopholes,
- Verification of data and developing temporary cache against malicious operations,
- Session inspection mechanism to stop attacks of hijacking and redo sessions,
- Boundary inspection, data encryption mechanism and resource access control to avoid leakage of privacy.

The IoT is vulnerable to a number of attacks that are mentioned in previous sections to disrupt the whole system, thus intrusion detection is a crucial concept for IoT deployments in real world such as industrial automation, building automation, smart metering and smart grids [58]. Attacks against a system are detected during analysis of actions in the system by a security mechanism broadly termed as Intrusion Detection System (IDS). When an attack is detected, IDS may log information about it and/or report an alarm. There are different existing intrusion detection techniques such as anomaly detection [59], data mining techniques [60] [61], statistical analysis [62] etc.

4. Conclusions

IoT is an emerging technology that has attracted a considerable number of researchers from all around the world. There have been major contributions making this technology adapted into our daily life. However, there are lots of key is-

sues addressing security concerns of IoT and they need more research effort to be solved.

In this paper, security concepts of IoT were reviewed substantially. Requirements and challenges of security measures in IoT were analyzed and collected under different headings. All kinds of security threats that may be critical in the development and implementation of IoT in different fields have been discussed and classified with respect to layers of IoT architecture: perception layer, network layer, support layer and application layer. Finally, the recent solutions have been provided for these threats and research directions with respect to security concerns have been introduced such as cryptographic mechanisms and firewalls.

References

[1] Madakam, S., Ramaswamy, R. and Tripathi, S. (2015) Internet of Things (IoT): A Literature Review. *Journal of Computer and Communications*, **3**, 164-173. https://doi.org/10.4236/jcc.2015.35021

[2] Tyagi, S., Darwish, A. and Khan, M.Y. (2014) Managing Computing Infrastructure for IoT Data. *Advances in Internet of Things*, **4**, 29-35. https://doi.org/10.4236/ait.2014.43005

[3] Gartner Inc. Press Release (2014) http://www.gartner.com/newsroom/id/2905717

[4] Gupta, J., Nayyar, A. and Gupta, P. (2015) Security and Privacy Issues in Internet of Things (IoT). *International Journal of Research in Computer Science*, **2**, 18-22.

[5] Yehia, L., Khedr, A. and Darwish, A. (2015) Hybrid Security Techniques for Internet of Things Healthcare Applications. *Advances in Internet of Things*, **5**, 21-25. https://doi.org/10.4236/ait.2015.53004

[6] Arseni, S.C., Halunga, S., Fratu, O., Vulpe, A. and Suciu, G. (2015) Analysis of the Security Solutions Implemented in Current Internet of Things Platforms. *IEEE Grid, Cloud & High Performance Computing in Science*, Romania, 28-30 October 2015, 1-4. https://doi.org/10.1109/ROLCG.2015.7367416

[7] Chandrakanth, S., Venkatesh, K. and Mahesh, J.U. (2014) Internet of Things. *International Journal of Innovations & Advancement in Computer Science*, **3**, 8.

[8] Shawish, A. and Salama, M. (2014) Cloud Computing: Paradigms. Inter-Cooperative Collective Intelligence: Techniques and Applications, Studies in Computational Intelligence 495, Springer-Verlag, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-35016-0_2

[9] Briseno, M.V., Hirata, F.I., Lopez, J.D.S., Garcia, E.J., Cota, J.N. and Hipolito, J.I.N. (2012) Using RFID/NFC and QR-Code in Mobile Phones to Link the Physical and the Digital World. InTech. https://doi.org/10.5772/37447

[10] Li, B.A. and Yu, J.J. (2011) Research and Application on the Smart Home Based on Component Technologies and Internet of Things. *Procedia Engineering*, **15**, 2087-2092. https://doi.org/10.1016/j.proeng.2011.08.390

[11] Ashton, K. (2009) That "Internet of Things" Thing. RFID Journal. http://www.rfidjournal.com/articles/pdf?4986

[12] National Instruments (2016) What Is a Wireless Sensor Network? http://www.ni.com/white-paper/7142/en/

[13] IEC Market Strategy Board (2014) Internet of Things: Wireless Sensor Networks. http://www.iec.ch/whitepaper/pdf/iecWP-internetofthings-LR-en.pdf

[14] Wang, R., Wang, J. and Wang, N. (2015) Analysis of Key Technologies in the

Internet of Things. 3*rd International Conference on Material, Mechanical and Manufacturing Engineering*, Guangzhou, 27-28 June 2015, 938-941. https://doi.org/10.2991/ic3me-15.2015.180

[15] An, J., Gui, X.L. and He, X. (2012) Study on the Architecture and Key Technologies for Internet of Things. *Advances in Biomedical Engineering*, **11**, 329-335.

[16] Huang, X., Craig, P., Lin, H. and Yan, Z. (2015) SecIoT: A Security Framework for the Internet of Things. *Security and Communication Networks*, **9**, 3083-3094. https://doi.org/10.1002/sec.1259

[17] Cloud Security Alliance (2015) Security Guidance for Early Adopters of the Internet of Things (IoT). https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf

[18] Suo, H., Wan, J., Zou, C. and Liu, J. (2012) Security in the Internet of Things: A Review. *IEEE International Conference on Computer Science and Electronics Engineering*, Hangzhou, 23-25 March 2012, 648-651. https://doi.org/10.1109/ICCSEE.2012.373

[19] Nguyen, K.T., Laurent, M. and Oualha, N. (2015) Survey on Secure Communication Protocols for the Internet of Things. *Ad Hoc Networks*, **32**, 17-31. https://doi.org/10.1016/j.adhoc.2015.01.006

[20] Yang, X., Li, Z., Geng, Z. and Zhang, H. (2012) A Multi-Layer Security Model for Internet of Things. *Springer International Workshop on Internet of Things*, Vol. 312, Changsha, 17-19 August 2012, 388-393. https://doi.org/10.1007/978-3-642-32427-7_54

[21] Farooq, M.U., Waseem, M., Khairi, A. and Mazhar, S. (2015) A Critical Analysis on the Security Concerns of Internet of Things (IoT). *International Journal of Computer Applications*, **111**, 1-6. https://doi.org/10.5120/19547-1280

[22] Qian, X. and Zhang, J. (2010) Study on the Structure of "Internet of Things (IOT)" Business Operation Support Platform. *IEEE International Conference on Communication Technology*, Nanjing, 11-14 November 2010, 1068-1071. https://doi.org/10.1109/ICCT.2010.5688537

[23] Weber, R.H. (2010) Internet of Things—New Security and Privacy Challenges. *Computer Law and Security Review*, **26**, 23-30. https://doi.org/10.1016/j.clsr.2009.11.008

[24] Chen, M., Wan, J.F. and Li, F. (2012) Machine-to-Machine Communications: Architectures, Standards and Applications. *KSII Transactions on Internet and Information Systems*, **6**, 480-497.

[25] Wind River Systems (2015) Security in the Internet of Things. http://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf

[26] European Commission. IoT Privacy, Data Protection, Information Security. http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1753

[27] ITU-T. Y.2060: Overview of the Internet of Things. http://www.itu.int/rec/T-REC-Y.2060-201206-I

[28] Mattern, F. and Floerkemeier, C. (2010) From the Internet of Computers to the Internet of Things. In: Sachs, K., Petrov, I. and Guerrero, P., Eds., *From Active Data Management to Event-Based Systems and More*, Springer, Berlin Heidelberg, 242-259. https://doi.org/10.1007/978-3-642-17226-7_15

[29] Mitrokotsa, A., Rieback, M.R. and Tanenbaum, A.S. (2009) Classifying RFID At-

tacks and Defenses. *Information Systems Frontiers*, **12**, 491-505. https://doi.org/10.1007/s10796-009-9210-z

[30] Borgohain, T., Kumar, U. and Sanyal, S. (2015) Survey of Security and Privacy Issues of Internet of Things. *International Journal of Advanced Networking Applications*, **6**, 2372-2378.

[31] Anwar, R.W., Bakhtiari, M., Zainal, A., Hanan, A.A. and Qureshi, K.N. (2014) Security Issues and Attacks in Wireless Sensor Network. *World Applied Sciences Journal*, **30**, 1224-1227.

[32] Deng, J., Han, R. and Mishra, S. (2005) Defending against Path-Based DoS Attacks in Wireless Sensor Networks. *ACM Workshop/Security of Ad Hoc and Sensor Networks*, Alexandria, 7 November 2005, 89-96. https://doi.org/10.1145/1102219.1102235

[33] Khoo, B. (2011) RFID as an Enabler of the Internet of Things: Issues of Security and Privacy. *IEEE International Conferences on Internet of Things, and Cyber, Physical and Social Computing*, Dalian, 19-22 October 2011, 709-712. https://doi.org/10.1109/iThings/CPSCom.2011.83

[34] Sharma, P., Saluja, M. and Saluja, K.K. (2012) A Review of Selective Forwarding Attacks in Wireless Sensor Networks. *International Journal of Advanced Smart Sensor Network Systems*, **2**, 37. https://doi.org/10.5121/ijassn.2012.2304

[35] Pooja, M. and Singh, Y. (2013) Security Issues and Sybil Attack in Wireless Sensor Networks. *International Journal of P2P Network Trends and Technology*, **3**, 7-13.

[36] Douceur, J.R. (2002) The Sybil Attack. *Springer International Workshop on Peer-to-Peer Systems*, Cambridge, 7-8 March 2002, 251-260. https://doi.org/10.1007/3-540-45748-8_24

[37] Ahmed, N., Kanhere, S.S. and Jha, S. (2005) The Holes Problem in Wireless Sensor Network: A Survey. *ACM SIGMOBILE Mobile Computing and Communications Review*, **9**, 4-18. https://doi.org/10.1145/1072989.1072992

[38] Kalita, H.K. and Kar, A. (2009) Wireless Sensor Network Security Analysis. *International Journal of Next-Generation Networks*, **1**, 1-10.

[39] Karlof, C. and Wagner, D. (2003) Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures. *Ad Hoc Networks*, **1**, 293-315. https://doi.org/10.1109/snpa.2003.1203362

[40] Kulshrestha, A. and Dubey, S.K. (2014) A Literature Review on Sniffing Attacks in Computer Network. *International Journal of Advanced Engineering Research and Science*, **1**, 2.

[41] Hermes Engineering. Security in Web Applications. http://www.hermes-ecs.com/en/page/59/documents

[42] OWASP, Internet of Things Project. https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project

[43] Zolanvari, M. and Jain, R. (2015) IoT Security: A Survey. http://www.cse.wustl.edu/~jain/cse570-15/ftp/iot_sec/index.html

[44] Sujitha, R., Raghavan, N.V., Suganya, K.S. and Devipriya, A. (2014) A Novel Survey on Internet of Things, Security and Its Application. *International Journal of Advanced Information and Communication Technology*, **1**, 8.

[45] Polk, T. and Turner, S. (2011) Security Challenges for the Internet of Things. http://www.iab.org/wp-content/IAB-uploads/2011/03/Turner.pdf

[46] Wander, A.S., Gura, N., Eberle, H., Gupta, V. and Shantz, S.C. (2005) Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks. *IEEE International*

Conference on Pervasive Computing and Communications, Kauai Island, 8-12 March 2005, 324-328. https://doi.org/10.1109/PERCOM.2005.18

[47] Miller, S.D. and Venkatesan, R. (2009) Expander Graphs Based on GRH with an Application to Elliptic Curve Cryptography. *Journal of Number Theory*, **129**, 1491-1504. https://doi.org/10.1016/j.jnt.2008.11.006

[48] Wood, A. and Stankovic, J. (2006) AMSecure: Secure Link-Layer Communication in TinyOS for IEEE 802.15.4-Based Wireless Sensor Networks. *ACM Conference on Networked Embedded Sensor Systems*, Boulder, 31 October-3 November 2006, 395-396. https://doi.org/10.1145/1182807.1182873

[49] Hu, W., Corke, P., Shih, W.C. and Overs, L. (2009) SecFleck: A Public Key Technology Platform for Wireless Sensor Networks. *Springer European Conference on Wireless Sensor Networks*, Cork, 11-13 February 2009, 296-311. https://doi.org/10.1007/978-3-642-00224-3_19

[50] Liu, D., Ning, P. and Li, R. (2003) Establishing Pairwise Keys in Distributed Sensor Networks. *ACM Conference on Computer and Communications Security*, Washington DC, 27-30 October 2003, 52-61. https://doi.org/10.1145/948109.948119

[51] Chung, A. and Roedig, U. (2008) DHB-KEY: An Efficient Key Distribution Scheme for Wireless Sensor Networks. *IEEE International Workshop on Wireless and Sensor Networks Security*, Atlanta, 29 September-2 October 2008, 840-846. https://doi.org/10.1109/MAHSS.2008.4660127

[52] Raza, S. (2013) Lightweight Security Solutions for the Internet of Things. No. 139, Mälardalen University Press Dissertations. http://www.diva-portal.org/smash/get/diva2:619066/FULLTEXT02.pdf

[53] The U.S. National Institute of Standards and Technology (NIST) (2012) Guide for Conducting Risk Assessments. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[54] The U.S. National Institute of Standards and Technology (NIST) (2002) Risk Management Guide for Information Technology Systems. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

[55] The International Standards Organization (ISO) (2009) The International Electrotechnical Commission (IEC). ISO/IEC 31010:2009 Risk management—Risk Assessment Techniques. http://www.iso.org/iso/catalogue_detail?csnumber=51073

[56] Jara, A.J., Ladid, L. and Skarmeta, A. (2013) The Internet of Everything through IPv6: An Analysis of Challenges, Solutions and Opportunities. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, **4**, 97-118.

[57] Zhang, W. and Baosheng, Q. (2013) Security Architecture of the Internet of Things Oriented to Perceptual Layer. *International Journal on Computer, Consumer and Control*, **2**, 2.

[58] Raza, S., Wallgren, L. and Voigt, T. (2013) SVELTE: Real-Time Intrusion Detection in the Internet of Things. *Ad Hoc Networks*, **11**, 2661-2674. https://doi.org/10.1016/j.adhoc.2013.04.014

[59] Verwoerd, T. and Hunt, R. (2002) Intrusion Detection Techniques and Approaches. *Computer Communications*, **25**, 1356-1365. https://doi.org/10.1016/S0140-3664(02)00037-3

[60] Patel, J. and Panchal, K. (2015) Effective Intrusion Detection System Using Data Mining Technique. *International Journal of Emerging Technologies and Innovative Research*, **2**, 6.

[61] Nguyen, H.A. and Choi, D. (2008) Application of Data Mining to Network Intrusion Detection: Classifier Selection Model. *Springer Asia-Pacific Symposium on*

Network Operations and Management: Challenges for Next Generation Network Operations and Service Management, Beijing, 22-24 October 2008, 399-408. https://doi.org/10.1007/978-3-540-88623-5_41

[62] Waskita, A.A., Suhartanto, H., Persadha, P.D. and Handoko, L.T. (2013) A Simple Statistical Analysis Approach for Intrusion Detection System. *IEEE Conference on Systems, Process & Control*, Kuala Lumpur, 13-15 December 2013, 193-197. https://doi.org/10.1109/SPC.2013.6735130