Security challenges in Internet of Things: survey

H.Reza Ghorbani, M.Hossein Ahmadzadegan
Department of Electrical Engineering and Informaion Technology Azad University of Tehran-Electronic Branch
Tehran, Iran
h.r.ghorbani@hotmail.com;m_ahmadzadegan@iauec.ac.ir

***Abstract*—The Internet of Things is part of our everyday life, which applies to all aspects of human life; from smart phones and environmental sensors to smart devices used in the industry. Although the Internet of Things has many advantages, there are risks and dangers as well that need to be addressed. The information used and transmitted on Internet of Things contain important info about the daily lives of people, banking information, location and geographical information, environmental and medical information, together with many other sensitive data. Therefore, it is critical to identify and address the security issues and challenges of Internet of Things. In this article, considering the broad scope of this field and its literature, we are going to express some comprehensive information on security challenges of the Internet of Things.**

***Index Terms*—Internet of Things, security, privacy, survey**

I. Introduction

Due to the expansion of internet in recent times and its being used in various devices and by humans, the scope of use of the internet of things is much broader than it could be imagined. According to forecasts by authentic IT companies, by 2020, the number of devices connected to the internet will exceed 50 billion. This large volume of devices connected to the internet denotes a much larger volume of information. Therefore, considering the nature of this information, which includes individuals' private information, bank account information, medical information, etc., it is crucial to examine the weaknesses and challenges in the security of these devices and secure the information against potential abusive practices. When it comes to using the Internet of Things, the security aspect is the greatest concern of devices that use the internet of things. The software data in internet of things might be personal, corporate or consumable; however, the stored data should be safe and secure against theft, manipulation and transport. Therefore, in order to elevate the security of internet of things, it is necessary to pay particular attention to the location of storage, media and method of transmission, the method of encryption, recovery and so on.

II. Definitions and standards

Still, there is no precise and general definition of Internet of Things which is universally accepted, and scholars and researchers, according to their field of research, have expressed their definitions with a few shortcomings. In the meantime, international organizations have given definitions for the Internet of Things, the most accepted and widely used of which, is the one defined by ITU in 2005. It is as follows: The Internet of Things is a global infrastructure for the information society that is able to provide advanced services through existing or evolving physical or virtual connections based on objects, compatible information and communication technologies. By expanding and developing the technology of the Internet of Things, each device in our environment will be able to communicate with another device and send information to them or control them, according to the information collected. The Internet of Things includes services and technology for connecting to objects on the internet and maintain the connection among distributed objects, which results in increased availability and provision of new services such as Wireless Sensor Networks (WSNs), which provides non-human-based services by connecting Physical discs and sensors of information technology and communication. Because of its vast field of activity, the Internet of Things has created its own organizations and standards, the most important of which can be referred to as follows in tabale 1: [2]- [17].

TABLE I
Used standards in IoT

organization	standards	year
Smart Homes	- Y.2060	2012
	- Y.2066	2014
	- Y.2068	2015
	- Y.2069	2012
ISO/IEC JTC 1	ISO/IEC JTC 1	2014
oneM2M	- TS0001-Functional Architecture	2015
	- TS0002-Requirements	2015
	- TS0003-Security Solutions	2015
	- TS0004-Service Layer Core Protocol Specification	2015
	- TS0005-Management Enablement(OMA)	2015
	- TS0006-Management Enablement(BBF)	2015
	- TS0009-HTTP Protocol Binding	2015
	- TS0010-MQTT Protocol Binding	2015
	- TS0011-Common Terminology	2015

III. Domain of Usage

Due to the expansion of technology and the increasing use of internet in all aspects of human life, the scope of use of the internet has become very broad and surpassed our imagination. In the table below, we refer to some functional areas of Internet of Things [18].

IV. Security of the Internet of Things

Security is a meaningful word for humankind. Since a long time ago, human beings have always sought to elevate their

978-1-5386-1971-1/17/$31.00 ©2017 IEEE

TABLE II
DOMAIN OF IOT USAGE

domains	example
Smart Homes	- Control and home security - Intelligent systems maintenance - Heating and cooling systems intelligent - Control and monitoring of energy consumption(water, electricity, gas)
Transportation	- Intelligent traffic control systems - Intelligent systems for maintenance of roads (land, air and sea) - Intelligent Systems Parking - RFID tags communication
Retail	- Supply Chain Control - Intelligent Shopping Applications - Smart Product Management
Agriculture	- Sensors check the soil moisture and temperature - Smart Irrigation
Factories and Industries	- Indoor Air Quality - Temperature Monitoring - Ozone Presence - Indoor Location - Vehicle Auto-diagnosis - Sensors check the soil moisture and temperature
Health Care	- Patients Surveillance - Sportsmen Care - Ultraviolet Radiation
Smart Cities	- Intelligent monitoring - Automatic transport - The exact energy management systems - Environmental monitoring
Wearable	- Smart Glasses - Smart clothes - Sleep Sensor - smart watch

level of security and all current laws and regulations have been created in order to enhance the security and comfort of human life. With the advent of technology and its increasing use by humans, security has gained a strong momentum for becoming a part of human priority and is considered before designing all technologies. The widespread use of the internet in many technologies has led to the creation of topics concerning the Internet of Things. All these technologies, including smart phones, smart sensors, Tracking systems and routers, traffic control systems, control and monitoring systems and cameras, intelligent health monitoring systems etc., have been designed and developed for human well-being. The fact that we use the Internet of Things in various areas such as banking, medicine, business, etc., and the importance of the information exchanged in these areas, as well as the importance of privacy for human beings, has led to the increasing significance of security in Internet of Things. Along with the correct use of this new technology and its tools and many of the benefits that have made it easy for human life, there are profitable cyber criminals who, given the very nature of the information exchanged in this area, have been subversive and exploited the weak spots of this new technology. This issue has made international organizations and institutions provide international protocols and standards in order to improve and enhance the security of this area. Hardware and processing constraints, limitations of power supplies, network infrastructure and communications, as well as heterogeneous devices, equipment and management of the internet domain, have limited the use of high-level encryption with overhead and high processing, therefore, we have to use cryptographic methods with overhead and low processing. The research done in this field is enormous and is trying to provide appropriate protocols and algorithms. However, due to the importance of security issue and in order to improve and enhance it's level, the research is still ongoing.

V. SECURITY CHALLENGES

One of the key challenges facing the realization of the Internet of Things is the security challenge, especially in the area of privacy and confidentiality among heterogeneous management and network capacity constraints. Reliability, economy, efficiency and effectiveness of the security and privacy of the Internet of Things are essential for ensuring confidentiality, integrity, authentication and access control. For example, users should be willing to share certain data about their habits in the public spaces of the internet, and this desire is created for the user only with the necessary safeguards to prevent the disclosure of information to other people. Therefore, the system must guarantee the privacy and confidentiality of the user. The rapid growth of the Internet of Things in the industry and technologies has led to new possibilities. However, given the vulnerabilities in intelligent home and car communications, people are not willing to put their security at risk. Therefore raising the level of security of the communications and ensuring its safety should be considered, which also requires an improvement in existing communication protocols safety or providing a new set of protocols with a higher safety level. These challenges in information management systems will serve as the basis for the law which, concerning the legal framework for information security and the privacy of the Internet of Things, should be determined and confirmed, since none of the traditional governmental regulations are proper for a global system such as the internet of things.

Therefore, due to the lack of unified laws and international standards, it is crucial to review and analyze existing protocols in order to upgrade them and integrate laws and standards among heterogeneous equipment in this area.

internet security challenges are categorized as follows:

A. *Implementation Challenges*

The Internet of Things is the domain where research is constantly fluctuating. Therefore, after doing some basic research in the technologies used in this field, it is necessary to introduce standards for design, operating system and communications, which form the basis for the development of services in this domain. The challenges that can be addressed in the implementation of the Internet of Things are as follows:

1) Security, privacy and confidentiality
   - Security itself faces challenges including:
     a) Securing the IoT's architecture.
     b) Active detection and protection of Internet of Things against attacks such as Dos and DDos.
     c) Standards, methods and tools for managing user identities and objects.

- In private domain:
    a) Personal information control.
    b) Improvement of privacy technologies and rules governing them.
    c) Standards, methods and tools for managing user identities and objects.
- In the domain of confidentiality:
    a) A more simple way is required for exchanging sensitive information, protecting them and keeping them confidential.
    b) Confidentiality should be a major component of the Internet of Things.

2) Standard
Heterogeneous management, heterogeneous program management, environments and devices, as well as the standardization of heterogeneous technologies, devices, applications, connections and communications, represent a major challenge.
3) Network communication constraints
The high degree of convergence caused by the devices connected to Internet of Things causes more delays and more permeability in the network infrastructure. Therefore, network infrastructure should provide security of communication and data transmission [1][25].

B. Privacy Challenges

Privacy concerns arise from the leakage of identity information that can be caused by knowing their personal data and identity and matching them to accessible data sources, For instance, it can be used to identify physically. Traditional methods such as random address or physical address hashing are there but not enough to maintain full privacy for users in internet communications. Nowadays, Cyber-attacks are well beyond attacks to physical layers or spheres and the attackers can discern the identity of users without knowing the physical address through eavesdropping the data packet along with the existing remote information.

The challenges of privacy are divided into two categories

- Data collection policies
- Data anonymity

In data collection policies, data access control and monitoring are actually implemented on the type of data and their quantity, and with these policies, the type of data can be collected, limited and controlled therefore as a result privacy will be guaranteed. In data anonymity, we discuss both data encryption and anonymity. The data can be anonymized through light encryption algorithms and appropriate designs, and concerning the connection, the discussion is related to eliminating any direct relationship between the data and its owner. There are also other important things such as:

- User privacy and data protection.
- Prevention of info leakage.
- Identification and matching of personal information [19] [20].

C. Network infrastructure challenges

The convergence resulted from objects connected to the Internet of Things has caused more demand for upgrading and coordination on the infrastructure of communication networks; the frequency of these messages causes latency and as a result the network becomes more vulnerable, thus, the network infrastructure has to ensure that the data is delivered safely. In this section, we also have the following categories for infrastructure challenges:

1) Hardware
The use of Internet of Things has been expanding in multiprotocol hardware, multi-standards, sensors, relays, and so forth, therefore, they will cause challenges.
2) Network connection
Connection to wireless network sensors on the Internet of Things that collect and analyze data, or the presence of Internet of Things in the ad-hoc network, monitoring of which is one of the challenges of the Internet of Things.
3) Architecture
The extranet architecture (external) on the internet makes it possible for a substantial collaboration between billions of objects. Single-domain systems will become multi-domain, which will cause new challenges.
4) Software and Algorithm
Software and algorithms such as super-algorithms that are installed on new cars and are self-learning can predict the user's route, are expanding in the field of Internet of Things. Therefore, the security of these systems is very important.
5) Compatibility
Due to the expansion of Internet of Things devices, data and data storage and international standards should always get an update so that the devices remain compatible.
6) Cloud computing and the Internet of Things
The widespread collecting, storing and analyzing of the data on the Internet of Things (such as sensors) has resulted in the effective use of cloud computing. Unauthorized access, retrieval and extraction of information from the cloud can be a challenge for the implementation of the Internet of Things [21][25].

D. Challenges Regarding the Quality of Service

According to previous literature, quality of service factors should be between three and eight, so in Internet of Things quality service models, objects are the only important and relevant factors.

1) Security
The privacy of individuals, their data, and behavioral patterns, etc, should be protected in Internet of Things in order to prevent abuse. Privacy policies focus on data processing, virtualization, and anonymity.
2) Performance
The function of the Internet of Things depends on many factors, such as the scale of the data in the system (for collecting sensor data) connected devices, cloud

performance in storage, network, signal strength, and so on.

3) Usability
Usability is an important factor in the quality of service the Internet of Things and is actually the ability of a product or system to achieve a goal. A system / product must have documentation, support and a simple user interface.

4) Reliability
Unbreakable activity for a specified period of time.

5) Stability
The ability of a system to maintain its performance under pressure.

6) Interoperability
The ability to communicate and exchange information with devices that belong to other networks.

7) Scalability
The ability to expand a system without affecting its performance.

The growth of the Internet of Things has affected appliances and accessories in a superb way and it will continue to expand. This also affects the human-computer interaction system and M2M, so the quality of any design for the systems and criteria used is very important by the quality factors [21][28].The challenges that the Internet of Things is facing and the standardization of its systems are constantly evolving so that it applies to the changes in technology and its field of application. Companies such as Cisco are working on self-regenerating hardware that can automatically correct the recognized errors. In the near future only one procedure can be seen for all errors or begin to save the defects and make a map out of it. A high quality model designed for such systems should include external factors like the power of signal, network connection.

E. Challenges Regarding Security Threats

Privacy for the person, business confidentiality and trustworthiness for the third person are the three main issues regarding the Internet of Things. Therefore, the Internet of Things should be able to withstand the threats of this domain. Given the previous vulnerabilities in common internet networks, Internet of Things now faces inactive (passive) and active attacks that disrupt its function easily and reduce the benefits of using Internet of Things and its services. Passive attacks are capable of retrieving information from the network and do not affecting its behavior. On the other hand, Active attacks directly impede the provision of services .we classify these threats into two types of external threats from outside the network and internal threats that are created within the network. given that internal threats know about valuable and confidential information available to the service, they are more dangerous compared to external threats [22].

F. Object Identification Challenges

The main challenge here is to identify the object. In order to ensure the integrity we have to use the naming method of architectural records. Although the DNS system provides the name translation service for internet users it is an unsafe naming system that can be targeted by attacks such as DNS cache poisoning and Man-in-the-middle, which inject fake DNS records into caches of victims. To overcome this problem, DNSSE, which is actually a DNS security, can be used to create the integrity and accuracy of the source record, and at the same time serve as a portable medium for distributing the public key of cryptography. We have to note that nothing has challenged DNSSE in the field of Internet of Things, and due to the high computation of communication overhead, it might not be appropriate for the Internet of Things [19].

G. Challenges Regarding Authentication and Authorization

Although public key encryption has already created advantages for authentication and authorization schemes, the lack of a reference to global certification has prevented the implementation of many theoretical plans in this area, because it will be challenging to design authentication systems without having a global certification. In this case, we have to consider other issues as well:

- Authentication and management.
- Trust management and integration policies.
- License and access control.
- End-to-end Security [19].

H. Light Cryptography and Security Protocols Challenges

Compared to the symmetric key encryption system, public key encryption has more security advantages but also a high overhead. Due to the hardware constraints on processing, storage, and power resources, this high overhead has become a challenge to its use. Reducing the overhead for public key cryptography and other complex security protocols are among the major challenges facing cryptography on the Internet of Things [19].

I. Software Vulnerability Challenges and Backdoor Analysis

Dynamic analysis of software is an effective approach in order to recognize the vulnerabilities; however, due to hardware and resource constraints it is useless. Therefore, we need behavioral simulation methods in the server and a powerful processing on them. Yet, the gap between the real devices and simulators has rendered this method difficult and challenging. On the other hand, dynamic analysis methods are a good and effective way for removing backdoors, yet, this is not a absolutely technical issue and management and policies play an important role. Revealing backdoors is very effective in reverse engineering and software inspecting [19].

J. Malware Challenges

Due to the change in the operating system's x86 architecture to Internet of Things platforms, conventional mechanisms against malware are practically no longer worthwhile, since processing power in Internet of Things devices has diminished; therefore, finding new methods and detecting malware has also created a new challenge in the domain of Internet of Things [19].

K. Related Challenges for the Android operating system

The Android operating system is a new and customized operating system from the core of Linux operating systems for Internet of Things, which has grown rapidly in the internet domain and has become very popular, yet, this operating system has its own weaknesses and pitfalls. Concerns about these issues have turned into challenges to the Internet of Things [19].

L. Security Challenges in Business

Businesses need to profit and grow capital in order to survive in their area of activity and this depends on security in the business. Business security can include security in the physical form, such as protecting the business from robbery, or in the form of information security such as keeping business innovation information or customer information secure. Therefore, security in business is very important and business executives spend a lot of money on security for their survival. On the other hand, with the growth of the Internet of Things in human societies and the involvement of this technology in human life, human business has also been influenced and uses Internet of Things for its own growth and development. The software data of internet of things in business usually concerns business-oriented data that are of high value due to the nature of business. Therefore, they should be safe and secure against theft, manipulation and transportation. Thus, we have to pay a special attention to the storage location, media and method of transmission, encryption, and retrieval, etc. to increase the security of Internet of Things. There are certain concerns in the business area as follows:

1) Insurance concerns
   Autonomous devices like smart cars have raised concerns about pricing for their insurance, but we have to note that their data is easier to evaluate. The data also need to be secure, so that the insurance assessments during accidents can be calculated based on actual and accurate data.
2) Lack of common standards
   The serious shortage of a unified and integrated standard for the Internet of Things and achieving a widespread industry is one of the challenges that the Internet of Things faces.
3) Social and legal concerns
   In spite of the expansion of the Internet of Things, there is still no mechanism for social and legal issues. [23]

The challenges of internet of things are not limited to the things mentioned above, and as the internet grows, things are changing and we can further investigate them. In addition, we can mention other challenges of the Internet of Things, such as:

- Setting the market up.
- Designing a more efficient architecture for the sensor network and storage of the collected data.
- Development of the mechanism for the processing and flow of collected data.
- Transmission to IPv6.
- Power sources of devices and sensors.
- Reduction of the costs of running the Internet of Things [1].

Security issues and challenges and privacy: given that they are linked with a huge amount of sensitive data, the security of internet of things must be considered very seriously because this environment is capable of physical attacks and should be protected against physical and malicious attacks. Categorization and classification of technologies belonging to internet of things, its objects, devices and services are expanding, so it is crucial to design an architectural standards that can perfectly support the abstract data model, interfaces and protocols with interconnected connections to support the widest domain possible that includes humans, creatures, objects, software, and so forth [22].

VI. SECURITY NEEDS FOR INTERNET OF THINGS

The devices of Internet of Things use many technologies, including communications, sensors, big data, etc., therefore, they have different security issues and because of the features of devices of Internet of Things such as low power consumption, light calculations, etc other issues emerge as well. In this section, we summarize the security needs of internet devices:

1) Lightweight Protocol and Encryption
   We have to select lightweight protocol and encryption in accordance to the device and the importance of the data, processing capabilities and power consumption of the device.
2) Communications Security
   The devices of internet of things can use communications such as short distance (Bluetooth), wireless, and wired. Therefore, security issues are required to support availability, confidentiality, authentication, and so on.
3) Data Protection
   The data on devices of internet of things can include user information, including physical information, locus of induction, user behavior, etc. Therefore, data must remain confidential until being sent to other devices or storage locations using appropriate encryption.
4) Physical protection
   Due to the ease of access to internet devices, we have to find a way in order to control physical access.
5) Identification and Allowing Access to Devices of Internet of Things
   We can add or reduce several devices of Internet of Things in the network, and each device has different licenses and domains. Therefore, it is necessary to identify and authenticate internet devices and permit the use of ID / password / MAC / certificate.
6) Monitoring and Controlling internet Devices
   Malware can damage, infect, or violated internet devices. Therefore, we need to control the activities of internet device in order to identify malicious behaviors [18].

VII. SECURITY REQUIREMENTS FOR INTERNET OF THINGS

Internet of Things has become one of the most important elements for the future of internet and has a great impact on social life and business environment. Many applications and services of internet of things are increasingly vulnerable to attacks or theft of information. To protect the Internet of Things from such attacks, we need advanced technologies in different areas. Identification, trust, and unification of data are among the particular key problems regarding the internet of things. The identification is required to connect two devices and exchange some public and private keys through knots in order to avoid data theft. The trust ability keeps unauthorized people from accessing data on the devices of internet of things. The unification of data will prevent any change in the data and assures that the incoming data to the receivers knot is unchangeable and transmitted by the sender. We can summarize other security requirements of the Internet of Things as follows:

- Lightweight and symmetrical solutions to support devices with limited resources.
- Lightweight keys management systems for reliable communication and distribution of encryption using communication and processing with minimal resources.
- Encryption techniques that can protect stored and shared data against other users' access.
- Techniques to support concepts such as identification, authentication and anonymity.
- Ability to store information using non-centralized computing and management key.
- Preventing the inference of spatial situation and personal information by observing commitments of Internet of Things [22][23].

VIII. Conclusion

While the notion of converging computers, sensors, and networks to monitor and control devices has been applied for years, the recent merger of key technologies and market trends is bringing about a new reality for the Internet of Things. IoT comes with a revolutionary, fully interconnected smart world, with relationships among objects and their environment and objects and people becoming more tightly intertwined. The future of the Internet of Things as a ubiquitous array of devices bound to the internet might alter how people think about what it implies to be online. While the potential ramifications are significant, a number of obstacles and challenges may stand in the path of this vision specifically in the areas of security; privacy; standards and interoperability; legal, regulatory together with the inclusion of emerging economies. The Internet of Things is about a complicated and evolving set of technological, social and political considerations across a diverse set of stakeholders. The Internet of Things is currently being utilized, and there is a demand to address its security challenges and maximize its benefits while reducing its risks. Therefore, this was the target of this paper, which has been realized.

References

[1] Mario Weber and Marija Boban, Security challenges of the Internet of Things, MIPRO 2016, May 30 - June 3, 2016, Opatija, Croatia.

[2] "ITU Internet Reports 2005: The Internet of Things, International Telecommunication Union.

[3] Y.2060-Overview of the Internet of Things, ITU-T, 2012.

[4] Y.2066-Common requirements of the Internet of things, ITU-T, 2014.

[5] Y.2068-Functional framework and capabilities of the Internet of Things, ITU-T, 2015.

[6] Y.2069-Terms and definitions of the Internet of Things, ITU-T, 2012.

[7] Internet of Things(IoT) Preliminary Report 2014, ISO/IEC, 2014.

[8] TS0001-Functional Architecture, oneM2M, 2015.

[9] TS0002-Requirements, oneM2M, 2015.

[10] TS0003-Security Solutions, oneM2M, 2015.

[11] TS0004-Service Layer Core Protocol Specification, oneM2M, 2015.

[12] TS0005-Management Enablement (OMA), oneM2M, 2015.

[13] TS0006-Management Enablement (BBF), oneM2M, 2015.

[14] TS0008-CoAP protocol Binding, oneM2M, 2015.

[15] TS0009-HTTP protocol Binding, oneM2M, 2015.

[16] TS0010-MQTT protocol Binding, oneM2M, 2015.

[17] TS0011-Common Terminology, oneM2M, 2015.

[18] Hyun-Jin Kim, Hyun-Soo Chang, Jeong-Jun Suh and Tae-shik Shon, A Study on Device Security in IoT Convergence, ICIMSA 2016, 23-26 May 2016, Jeju, South Korea.

[19] Zhi-Kai Zhang, Michael Cheng Yi Cho, Chia-Wei Wang, Chia-Wei Hsu, Chong-Kuan Chen and Shiuhpyng Shieh, IoT Security: Ongoing Challenges and Research Opportunities, 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications, 17-19 Nov. 2014, Matsue, Japan.

[20] Hsin Chung Chen, Mohammad Abdullah Al Faruque and Pai H. Chou, Security and Privacy Challenges in IoT-Based Machine-to-Machine Collaborative Scenarios, CODES/ISSS 16, 01-07 October 2016, Pittsburgh, PA, USA.

[21] Jay Kiruthika and Souheil Khaddaj Software Quality Issues and Challenges of Internet of Things, 2015 14th International Symposium on Distributed Computing and Applications for Business Engineering and Science, 18-24 Aug. 2015, Guiyang, China.

[22] Mohamed Abomhara and Geir M. Kien Security and Privacy in the Internet of Things: Current Status and Open Issues, 2014 International Conference on Privacy and Security in Mobile Systems (PRISMS), 11-14 May 2014, Aalborg, Denmark.

[23] Sachchidanand Singh and Nirmala Singh Internet of Things(IoT): Security Challenges,Business Opportunities Reference Architecture for E-commerce, 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), 8-10 Oct. 2015, Noida, India.

[24] Imen Ben Ida, Abderrazak Jemai and Adlen Loukil, A survey on security of IoT in the context of eHealth and clouds,2016 11th International Design Test Symposium (IDT), 18-20 Dec. 2016, Hammamet, Tunisia.

[25] Se-Ra Oh and Young-Gab Kim, Security Requirements Analysis for the IoT, 2017 International Conference on Platform Technology and Service (PlatCon), 13-15 Feb. 2017, Busan, South Korea.

[26] Aditya Parashar and Sachin Rishishwar, Security Challanges In IoT, 2017 Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), 27-28 Feb. 2017, Chennai, India.

[27] Kewei Sha, Ranadheer Errabelly, Wei Wei, T. Andrew Yang and Zhiwei Wang, EdgeSec: Design of an Edge Layer Security Service to Enhance IoT Security, 2017 IEEE 1st International Conference on Fog and Edge Computing (ICFEC), 14-15 May 2017, Madrid, Spain.

[28] Pal Varga, Sandor Plosz, Gabor Soos and Csaba Hegedus Security Threats and Issues in Automation IoT, 2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS), 31 May-2 June 2017, Trondheim, Norway.