The European Proceedings of
Social and Behavioural Sciences
EpSBS

www.europeanproceedings.com
e-ISSN: 2357-1330

DOI: 10.15405/epsbs.2020.10.03.133

ICEST 2020

International Conference on Economic and Social Trends for Sustainability of Modern Society

PROBLEMS OF SECURITY FOR THE IMPLEMENTATION OF THE INTERNET OF THINGS

Alena Fomina (a), Yulia Antokhina (b), Elena Semenova (c)*
*Corresponding author

(a) CRI Electronics, 12, Kosmonavta Volkova Str., MGIMO University, 76, Prospect Vernadskogo, Moscow, Russia, fomina_a@instel.ru
(b) State University of Aerospace Instrumentation, 67, Bolshaya Morskaya Str., Saint-Petersburg, Russia, antoxina@guap.ru
(c) State University of Aerospace Instrumentation, 67, Bolshaya Morskaya Str., Saint-Petersburg, Russia, egsemenova@mail.ru

Abstract

Internet of Things (IoT) deployment and security issues are closely intertwined. In this area, there are at least two levels of questions and problems. The first level is the responsibility of governments and international organizations. It addresses the issues of regulating activities in IoT, creating the most favorable conditions for business, ensuring the security of stored and transmitted data belonging to various market players. Security issues include not only identifying various vulnerabilities, but also countering cybercrime and enemy states. The second level covers a wide range of issues related to the development of necessary devices, equipment, networks, their architectures and related software. In addition, issues of power consumption of IoT and power of remote IoT devices, development of algorithms and means of detecting illegal access attempts and countering of them is very important. In terms of providing communication and significantly improving its quality, the development of IoT technologies is closely related to the development of 5G technologies, especially mmWave. The features and advantages of the article include a comprehensive review of all the mentioned issues. Such an approach helps not only deeper and from all sides to consider the situation with the development and deployment of IoT. It also provides an opportunity to assess the development prospects of IoT, communications technology, connectivity and security.

Keywords: Deployment, development, IoT, laws, security.

https://doi.org/10.15405/epsbs.2020.10.03.133
Corresponding Author: Elena Semenova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

1. Introduction

As Industry 4.0 implements an increasing number of business processes, government functions, monitoring of the critical life support structure, defense and national security issues are carried out online. All these tasks are provided by high-speed Internet technologies, which at the same time represent the main source of threats to digital transformation (McGrath et al., 2019). Governments of various countries and interstate entities (EU) are developing various measures to ensure the security of the Internet of Things (IoT), including industrial IoT (IIoT) (MEPs Adopt Cybersecurity Act and Want EU to Counter IT Threat from China, 2019; Fuller, 2019).

The safe functioning of IoT requires the implementation of a wide range of activities - from the search for more advanced materials for the manufacture of power supplies and electronic components to the creation of integrated circuits (IC), functional units, infrastructure, architectures and protocols for the safe exchange of data in IoT.

Nowadays, researchers all around the world are actively looking for new ways to use the energy of radio waves of wireless networks to power remote IoT sensors, which will eliminate batteries, reduce the cost, size and weight of electronic devices (MEPs Adopt Cybersecurity Act and Want EU to Counter IT Threat from China, 2019; Fuller, 2019). Work is also underway to create memory for artificial intelligence (AI) and IoT (Dahad, 2019). Of great importance for the development of IoT and ensuring its safety is the human-machine interface (HMI) (Ramakrishnan, 2020). An important role in the deployment of IoT and IIoT is played by MCU with machine learning (ML) (Ramakrishnan, 2020), as well as 5G. Thus, general IoT security issues find concrete solutions (Army Researchers Identify New Way to Improve Cybersecurity, 2019).

2. Problem Statement

The problem of IoT development is connected both with issues falling within the competence of state authorities, and with issues whose solution depends directly on suppliers of electronic components and functional nodes, network equipment, software, design tools, architecture developers, communication operators, etc.

Governments and businesses all around the world, because of development of IoT and related technologies, are confronted with security issues. Threats come from hackers and criminal groups, including terrorists, but the most dangerous ones come from specific states. For example, the EU considers threats posed by China's growing technological presence on its territory to be serious. It is assumed that Chinese laws on state security, which oblige private companies to cooperate with the government, including outside the country, pose a threat to EU cybersecurity (MEPs Adopt Cybersecurity Act and Want EU to Counter IT Threat from China, 2019). In addition to the adoption of laws governing the activities of all players in the field of IoT, it is important to train the necessary personnel, also those in the field of cybersecurity. To address everyday issues related to the development and security of IoT, governments of various countries create specialized departments with monitoring functions, develop and implement strategies and programs in this area (Fuller, 2019).

https://doi.org/10.15405/epsbs.2020.10.03.133
Corresponding Author: Elena Semenova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

The development of IoT and its security require solving many problems. First, the creation of new materials and the improvement of energy collection methods, as well as the creation of devices based on them that can stimulate the mass distribution of IoT sensors that do not use batteries (Nelson, 2019). Secondly, this is the identification of the mechanism of influence of IoT on energy consumption and the solution of problems arising in connection with this. Thirdly, there is an ever-increasing need for all large amounts of memory and the creation of non-volatile high-capacity memory circuits for AI and IoT tools (Dahad, 2019). Fourth, in the Industry 4.0 era, HMIs are ubiquitous, becoming more portable and mobile. The sizes of electronic IoT devices are small, therefore, in order to ensure easy integration, HMI for them should also be small (Ramakrishnan, 2020). Fifth, MCU with ML plays an important role in deploying IoT and IIoT. Experts believe that the first MCU with ML engines will appear within 2-3 years, and killer apps - in the next 3-5 years. Sixth, the development of digital innovation has led to increased requirements for network performance - today it is much more than just the transfer of audio and video data over the Internet. The most advanced digital environments use hyperconnectivity and hyperscalability to provide ultra-fast collection, processing and transmission of astronomically huge data sets, high speed of implementation and unprecedented consumption of online services by users. Seventh, with the further development of IoT, 5G communication technologies, especially mmWave and MIMO technologies, which will ensure the ability of new generation networks to process the entire amount of IoT data, will be of great importance. Many experts believe that the creation of private 5G networks operating in factories will have the greatest impact on IIoT. The task of scaling both IoT and IIoT requires the transfer of information processing functions to peripheral sections of the network. The traditional way of transmitting data from sensors to a centralized server and vice versa slows down the decision-making process, regardless of the achieved transmission rate (Browne, 2019). Finally, the existing cybersecurity systems of IoT and networks in general do not meet continuously strengthening requirements. Systems are required that can effectively counteract cyber attacks: capture all threats, provide sufficient analysis of network activity, separate real threats from warnings, which in reality are not worth serious threats (Army Researchers Identify New Way to Improve Cybersecurity, 2019).

3. Research Questions

Research questions include:

- General IoT security requirements;
- National legislation of the EU, UK and USA regarding IoT;
- UK National IoT Security Agencies;
- UK National IoT Strategy;
- UK policy on personnel training for IoT security;
- Research in the field of energy supply IoT;
- New RRAM technology to support AI in IoT and edge computing;
- Increased memory capacity in systems with HMI;
- Development perspective of MCUs with edge AI engines;
- Hyperscale computing and need for development of security processors;

https://doi.org/10.15405/epsbs.2020.10.03.133
Corresponding Author: Elena Semenova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

- 5G nets processability of full IoT traffic;
- Private 5G nets as a factor of IIoT development;
- The role of 5G nets in IIoT development;
- A method of improvement of network security.

4. Purpose of the Study

The purpose of the study is to obtain specific data on all issues raised in the study.

In the block within the competence of national governments and interstate associations - the establishment of general IoT security requirements; specific laws of the EU, UK and USA regarding IoT. A UK case study of IoT security agencies, a national IoT strategy, and IoT security training policies.

In terms of the competence of industrial corporations and research organizations, the purpose of the study is:

- The work of the Massachusetts Institute of Technology (MIT) and the Wiliot startup in the field of energy supply IoT;
- New RRAM technology from CEA-Leti and Stanford University to support AI in IoT and edge computing;
- The work of Cypress Corporation to increase memory capacity in systems with HMI;
- Development perspective of MCUs with edge AI engines by several MCUs providers and ARM;
- Hyperscale computing and need for development of security processors (based on examples from the activities of Apple, Google, Microsoft and Amazon);
- Work in the field of interaction of IoT, IIoT and 5G nets;
- The new method of improvement of network security, developed by ARL and Towson University.

5. Research Methods

In the article, based on the collection, analysis and generalization of information related to research issues, the methods of botton-up analysis and top-down analysis were used.

Top-down analysis has been applied to issues within the competence of the EU, UK and US government bodies.

Botton-up analysis has been applied to issues related to the competence of industrial corporations and research organizations.

6. Findings

General IoT Security Requirements. Until recently, there were few points of entry for malware: an open port on the network, or via email. Even now, phishing remains an extremely effective way of hacking security systems: up to 95% of violations are associated with it. Today, the number of potential channels for cyber attacks is increasing: they include messaging services, as well as shared drives, mobile devices, and collaboration applications (Dropbox, Slack, Salesforce, etc.). Traditional cybersecurity tools - anti-

https://doi.org/10.15405/epsbs.2020.10.03.133
Corresponding Author: Elena Semenova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

malware systems, firewalls, sandboxes - are no longer able to provide effective protection against existing threats. New cybersecurity issues require new security models to replace traditional ones. One of the most effective approaches is connected with researching not the threat itself in the form of malware, but its sources. Accordingly, the use of automated solutions in the field of cybersecurity is required, which makes it possible to fully use the advantages of digital transformation.

National laws of the EU, UK and USA regarding IoT. In 2019, the European Union Cybersecurity Act was adopted in the EU, which established the first certification scheme for products, processes and services sold in the EU for compliance with cybersecurity standards. Based on the EU Cybersecurity Act certification of connected devices is carried out. The law extends the authority of the European Union Agency for Cybersecurity (ENISA). The purpose of the adoption of the Law is to provide the EU with the opportunity in the long term to counter security threats against the backdrop of the development of digital technologies (MEPs Adopt Cybersecurity Act and Want EU to Counter IT Threat from China, 2019). In 2018, the UK government issued the Code of Practice (CoP) for the Internet of Things security, according to which manufacturers should provide for the possibility of ensuring security at the stage of creating their products, and not eliminate the problems that arise exclusively on software update level. In the United States, the IOT Consumer TIPS Act of 2017, the SMART IoT Act of 2018 and the Internet of Things (IoT) Cybersecurity Improvement Act of 2019 have been adopted (Hashemi et al., 2016).

UK National IoT Security Agencies. In the UK, the National Cyber Security Center (NCSC), established in October 2016, is responsible for protecting Internet activities. Since then it has prevented more than 1,000 significant cyber incidents. The introduction of the 5G standard enhances the role of the safety factor in managerial decision-making, and new challenges must be addressed globally. Another significant factor in the development of Internet technologies is the methods of protecting the user's personal data. One of the tasks of NCSC is the creation of technical solutions to enhance security when working on the Internet. So, within the framework of the Active Cyber Defense program, a system was developed that is able, using data on potential threats, to block connections with malicious sites in government networks. Under the protection of the system - about 1.3 million users of state resources. At the end of 2018, 54 million malicious connections were blocked, while about 11 thousand unique malicious domains were blocked monthly (Tayyaba et al., 2017).

Another NCSC project is the creation of an anti-spoofing mechanism that protects state-owned brands. Through its introduction, Her Majesty's Revenue and Customs (HMRC) in one year was able to prevent about 500 million attacks. 2.5 years ago, NCSC developed a system to automatically remove phishing sites. As a result, the time to eliminate threats of this type was reduced, and over the past period, the share of the United Kingdom in global phishing fell from 5.3 to 2.2%).

UK National IoT Strategy. In the UK, the importance of IoT cybersecurity is noted in the State Industry Development Strategy, the National Cybersecurity Program and the National Cybersecurity Strategy (was published in 2016 and is designed for the period until 2021, was revised in 2019).

UK IoT Security Training Policy.

To ensure the sustainable development of the country after 2021, a Strategy for the development of skills in the field of cybersecurity was prepared, designed to respond to existing challenges related to training. The implementation of the Strategy involves the dissemination of information on the prospects

https://doi.org/10.15405/epsbs.2020.10.03.133
Corresponding Author: Elena Semenova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

and attractiveness of the cybersecurity sphere, as well as on existing career opportunities among the widest sections of the population with the help of independent specialists. In 2019, it is planned to launch the updated CyberFirst mechanism. If earlier it was intended to provide assistance to students who decided to choose cybersecurity as the direction of training (scholarships, internships), now under this brand all possible tools to help people who decide to master cybersecurity skills, regardless of age and professional, will be combined and unified experience. The brand will be available not only for state, but also for private initiatives: companies can use it for their own events aimed at popularizing the sphere of cybersecurity (Al-Bahri et al., 2019).

The government has introduced a number of measures aimed at increasing the number of professionals and training areas in the field of cybersecurity. One of the long-term initiatives is the Cyber Discovery program with a budget of £ 20 million, aimed at attracting young people to cybersecurity, identifying and training talented specialists. Also, a program was launched to finance the implementation of initiatives of educational institutions for training specialists in the field of cybersecurity using the Cyber Skills Immediate Impact Fund (CSIIF), as well as a scholarship program for graduates of universities specializing in cybersecurity (Yavari et al., 2017).

IoT Energy Research. Four mechanisms of the impact of IoT on energy consumption are distinguished:

- Direct (local) impact of IoT components on energy systems;
- Remote energy consumption by IoT infrastructure;
- Energy consumption in the manufacturing process of IoT devices;
- Indirect impact of IoT on energy systems through changes in consumer behavior associated with an increase in the number of devices used and the volume of services consumed. For the sustainable development of IoT, there are many solutions in the field of energy supply. For example, the Massachusetts Institute of Technology (MIT) proposed using flexible “rectennas” (the AC-signal-to-DC-power devices) made from a thin layer of molybdenum disulphide for energy. Such a device is capable of efficiently generating direct current from a wireless network: a 150 μW Wi-Fi signal converts to 40 μW of electricity - this amount is sufficient to power IoT devices. Another MIT project involves the collection of energy generated by daily fluctuations in ambient temperature.

New RRAM technology for AI support in IoT and edge computing. CEA-Leti and Stanford University creates new non-volatile memory (NVM) technology - ENDURER RRAM. It helps overcome the challenges of previous generations of NVM. The multilevel-cell RRAM has a 10-year lifespan and is suitable for a wide range of applications - machine learning, management, security and cryptography. The new IC provides (with the same speed) 10 times better energy efficiency compared to the standard built-in flash memory due to low working power consumption, as well as ultra-fast and energy-efficient transitions from on to off and vice versa. Its main purpose is AI and IoT (Dahad, 2019).

Increased memory capacity on systems with HMI. In the Industry 4.0 age the HMIs are ubiquitous, becoming more portable and mobile. The IoT electronic devices are small in size; therefore, in order to ensure easy integration, HMI for them should also be small. Thus, there is a strong need to reduce the size

https://doi.org/10.15405/epsbs.2020.10.03.133
Corresponding Author: Elena Semenova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

of the HMI circuit board. Traditionally, HMIs are controlled by MCU, MPU, or FPGA, and use SDRAM or PSRAM to execute code and buffer graphics. This approach, however, is highly unprofitable from the point of view of simplicity of design, power consumption and the occupied space of the HMI system. An alternative approach to optimizing system design is to use HyperRAM (pseudoSRAM). HyperRAM offers a high throughput of 400 MB / s (3200 Mb / s), comparable to the bandwidth of SDR SDRAM, DDR SDRAM or Parallel ADMUX pseudoSRAM. Nevertheless, it is small in size (area up to 48 mm2) and has only 12 contacts for data transfer. In addition, this approach can significantly increase the memory capacity of HMI (Ramakrishnan, 2020).

Development perspective of MCUs with edge AI engines. Most well-known suppliers of microcontrollers, such as NXP, Renesas and STMicroelectronics, believe that ARM core Cortex-M processor cores are best suited to realize the capabilities of micro machine learning (TinyML technology). MCUs with edge AI engines are designed for resource-limited environments. Targeted market for MCUs with edge AI engines is IoTwith AI (AIoT). The AIoT sector potentially covers billions of devices. The problem with developers is that they cannot afford to spend time and money developing individual solutions for each application. Accordingly, flexibility and ease of use are absolutely paramount. The choice of ARM solutions is logical - there is an ecosystem and tools that allow customers to easily quickly develop products and quickly bring them to the market (without big expenses for customization).

An alternative approach is to use the RISC-V ISA. On the one hand, this open source ISA allows you to design processors without a license fee, and on the other hand, projects based on the RISC-V ISA are protected no worse than any other type of intellectual property. In addition, designers can choose add-on extensions, as well as add their own individual extensions.

Hyperscale computing and need for development of security processors. Advanced R&D in various industries require tremendous processing power and data volumes to support modeling and analysis. Dynamic e-commerce and huge multi-player gaming environments rely to the same degree on hyperscale architectures to deliver unrivaled customer service. Financial institutions need an environment that allows them to conclude a multitude of trading transactions almost instantly, while scalable Internet services require speed and expandability. Many corporations, including Apple, Google, Microsoft and Amazon, have begun to create their own hyperscale processors.

Without specially designed security processors for organizations that rely on digital innovation, the choice is small: slow down, taking into account security constraints, or not protect their environment at all. In an era when cybersecurity threats are constantly changing, leaving critical processes open or at best barely protected by outdated measures like access control lists is simply unacceptable. After all, when a variety of advanced network functions are combined into the next-generation intelligent infrastructure, the absence of viable security tools that can protect and verify hyperspeed, hyperconnected and hypersized environments will lead to a crisis that will be very difficult to resolve if not impossible.

It is important, that the Internet of Things changes the security industry. The IOT itself can allow various data to be transferred seamlessly among physical devices directly to the Internet. The number of smart devices is growing and will create a new network with information that allows supply chains to assemble and communicate in new ways. The Gartner prospects more than 26 billion installed units on the Internet of Things (IoT) by 2020 (Singh & Singh, 2015).

https://doi.org/10.15405/epsbs.2020.10.03.133
Corresponding Author: Elena Semenova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

We live in the time, when lots of mobile devices are connected and offer new types of applications. The IoT changes so fast and the runtime interactions among devices and applications put special requirements on the systems' architecture (Alkhabbas et al., 2017).

Among the newest ways of use we should note the multilayered method for securing data transport from a cellular connected Internet of Things device to a host through a cellular network. This particular method uses interlocking security elements, which, when implemented in their totality, provide a highly secure connectivity solution (Lee & Fumagalli, 2019).

Also, we should note, that wearable devices present an increasingly attractive solution for various applications in different fields from the military to consumer electronics. They will also play an integral role in the 5G networks, which are expected to operate with higher bit rates and lower outage probabilities in smaller microcells covering broader areas than 4G (Aun et al., 2017).

On 5G nets processability from IoT traffic. With the further development of IoT, 5G communication technologies, especially mmWave and MIMO technologies, which will ensure the ability of new generation networks to process the entire amount of IoT data, will be of great importance. 5 G technologies will be a driving factor in growth opportunities in all end markets (Figure 1). Components demanded by major communication carriers include mmWave devices, such as amplifiers, antennas, waveguide loads, ADC and DAC. The result of the transition to MIMO technology and the reduction of communication nodes has become the need for miniaturization and integration of components. As a result, compact subsystems are located in a small package of the network node, providing high bandwidth and wide wireless coverage (Browne, 2019).

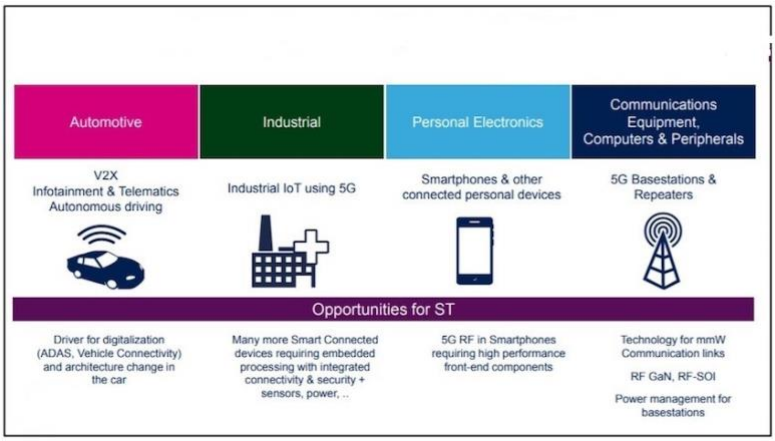

Figure 01. 5G Will Drive Growth Opportunities in all End Markets

Private 5G nets as a factor of IIoT development. The greatest impact on IIoT of things will be the creation of private 5G networks operating in factories. Companies will be able to create secure dedicated networks in limited geographical areas, adapting them to specific industrial applications.

For the first time, a fundamental opportunity appears for both enterprises and smart cities to deploy their own network, which allows introducing various innovations. Experts emphasize that spectrum security for private 5G networks will continue to be costly, but the new deployment model will be significantly different from the current model for private networks, which requires long-term transactions with telecom operators.

https://doi.org/10.15405/epsbs.2020.10.03.133
Corresponding Author: Elena Semenova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

Industrial players introducing 5G private networks for IIoT will be able to plan their network for a period of 10-15 years, knowing that they have a certain spectrum. Thus, private 5G networks are really a very big innovation, with the potential to completely change the dynamics of factory networks.

The role of 5G nets in IIoT development. Verizon Communications predicts, by 2035, 5G IIoT will generate $ 12.3 trillion in global economic revenues and support 22 million jobs. Digitalization of transport, agriculture and other sectors of the real sector will be implemented.

According to IDC forecasts, in the coming years, the bulk of the costs of production, transport and housing and communal services will be associated with the implementation of the Internet of things technologies - with special attention to the management of production facilities, vehicles and freight transportation. In just the next two years, the industrial Internet of things will attract $ 300 billion, which is twice as much compared to the consumer segment. All this will contribute to Industry 4.0 development.

ARL's method of improvement of network security. A common type of cybersecurity system is distributed network-based intrusion detection system (figure 2). Their use allows a small number of highly qualified specialists to control several networks simultaneously, while ensuring cost savings due to economies of scale and a more efficient allocation of resources. The limitation of such systems is that the transfer of the entire amount of data from intrusion detection sensors with which the protected network is equipped to central analyzers requires too large bandwidth. Therefore, most modern distributed intrusion detection network systems provide cybersecurity professionals with partial data, sending them only threat warnings or summaries of actions.

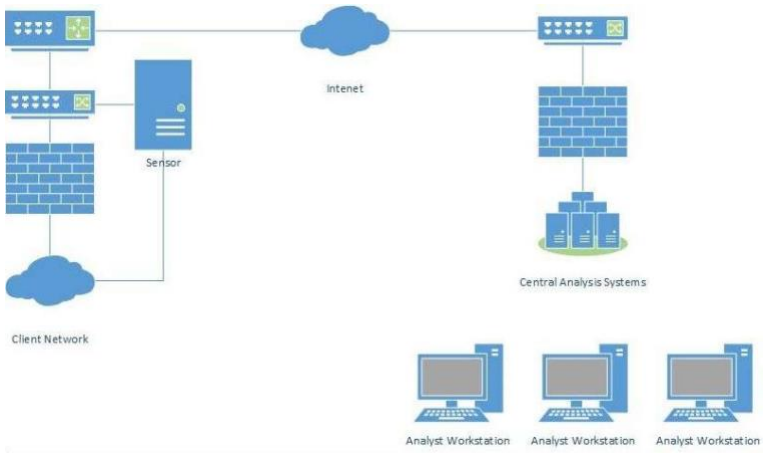

Figure 02. Detection of invasions on distributed networks base

To overcome this problem, the Army Research Laboratory (ARL) and Towson University have created a method of maximum compression of network traffic without losing the ability to detect and analyse malicious activity. The developed strategy is effective for reducing the amount of network traffic transmitted from the sensors of the protected distributed network to the central analytical system, and is promising for improving the reliability and security of US military networks. ARL and Towson University plan to continue the study. Their new goal, based on the joint use of network traffic compression methods and network classification, to ensure that the volume of traffic required for transmission to central analytical

https://doi.org/10.15405/epsbs.2020.10.03.133
Corresponding Author: Elena Semenova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

systems is reduced to less than 10% of the initial volume with allowable loss of warnings not exceeding 1% (Army Researchers Identify New Way to Improve Cybersecurity, 2019).

7. Conclusion

The problems, that arise when deploying of IoT and ensuring its security, are completely solvable. Moreover, these issues are solved both at the level of national governments (interstate associations) from one side, and industry and the scientific community from another side. The legislative measures, which adopted or being under developing by the authorities of different countries mostly fully meet the needs of IoT development and security. The most important is to note that in the process of drafting such laws, not only the current situation should be taken into account, but also the prospects for development.

This predictive approach is very promising. An important case is that legislation and various government initiatives are constantly adjusting to reflect the changing environment. As can be seen from the example of the UK, there is already a sufficient infrastructure of bodies implementing public policy in the field of IoT. One of the main components of this policy is the training of personnel intended for both the deployment and implementation of IoT, and for ensuring its security.

It is necessary to note that the activities of industry and the scientific community in the field of IoT cover all possible aspects of its development and security. At the same time, this comprehensive approach, starting with the issues of creating inexpensive and reliable power sources, ends with the development of methods for ensuring safety of activities in the IoT.

Concerning the development of power supplies, special attention should be shown to energy harvesting devices that can serve remote Autonomous points of IoT networks without using stationary power grids. And about the development of hardware, attention is needed to increasing the capacity and reliability of memory (mostly non-volatile), performance of MCU, MPU, FPGA and etc. Edge AI, HMI, hyperscale computing, and cryptography technologies play an increasing role in deploying IoT networks and ensuring their security.

The development of IoT technologies closely tied to the development of 5G technologies. They are mutually complementary. It is possible to deploy the most productive and secure IoT networks based on 5G networks, especially using mmWave technology. At the same time, the proliferation of IoT networks is driving demand for 5G devices, networks, and technologies.

In conclusion, it is necessary to note that IoT, including IIoT, is one of the transformational technologies that can significantly change the way of life of humanity.

References

Al-Bahri, M., Kirichek, R., & Borodin, A. (2019). Integrating Internet of Things with the digital object architecture. Internet of Things, Smart Spaces, and Next Generation Networks and Systems 2019. In 19*th International Conference On Next Generation Teletraffic And Wired/Wireless Advanced Networks And Systems (New2an), And The 12th Conference On Internet Of Things And Smart Spaces (Rusmart).* (pp. 540-547). https://doi.org/10.1007/978-3-030-30859-9_47

Alkhabbas, F., Spalazzese, R., & Davidsson, P. (2017). Architecting Emergent Configurations in the Internet of Things. 2017 IEEE International Conference on Software Architecture (ICSA). Gothenburg, Sweden. IEEE. https://doi.org/10.1109/ICSA.2017.37

Army Researchers Identify New Way to Improve Cybersecurity (2019, April 17). Phys.org. https://phys.org/news/2019–04-army-cybersecurity.html

Aun, N., Soh, P., & Al-Hadi, A. (2017). Revolutionizing Wearables for 5G: 5G Technologies: Recent Developments and Future Perspectives for Wearable Devices and Antennas. *IEEE Microwave Magazine, 18*(3), 108 – 124. https://doi.org/10.1109/MMM.2017.2664019

Browne, J. (2019). Can 5G Handle Next-Gen Data? Electronic Design. https://www.electronicdesign.com/industrial-automation/can5g-handle-next-gen-data

Dahad, N. (2019, February 26). NVM ReRAM Memory Cell Targets Edge AI. EE Times. https://www.eetimes.com/document.asp?doc_id=1334371

Fuller, K. (2019). Security Technology Is Not Enough. https://www.theengineer.co.uk/cyber-security/

Hashemi, S. M., & He, J., Basabi, A. E. (2016). Security For The Internet Of Things With Intelligent Automata. 2nd IEEE International Conference On Computer And Communications, ICCC 2016 Chengdu. https://doi.org/10.1109/CompComm.2016.7924864

Lee, C., & Fumagalli, A. (2019). Internet of Things Security - Multilayered Method For End to End Data Communications Over Cellular Networks. 2019 IEEE 5th World Forum on Internet of Things (WF-IoT). IEEE. https://doi.org/10.1109/WF-IoT.2019.8767227

McGrath, S., Zhao, X. F., Qin, Z. Z., Steele, R., & Benedetti, A. (2019). One-sample aggregate data meta-analysis of medians. *Statistics in Medicine, 38*, 969– 984. https://doi.org/10.1002/sim.8013

MEPs Adopt Cybersecurity Act and Want EU to Counter IT Threat from China (2019, March 20). European Parliament News. http://www.europarl.europa.eu/news/en/press-room/20190307IPR30694/meps-adopt-cybersecurity-act-and-want-eu-to-counter-it-threat-from-china

Nelson, P. (2019). Power over Wi-Fi: The End of IoT-Sensor Batteries? Network World. https://www.networkworld.com/article/3342417/internet-of-things/power-over-wi-fi-the-end-of-iot-sensor-batteries.html

Ramakrishnan, V. (2020). Expansion Memory in Industrial and Consumer HMI systems. EETimes magazine. https://www.eetimes.com/expansion-memory-in-industrialand-consumer-hmi-systems/

Singh, S., & Singh N. (2015). Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce. 2015 International Conference on Green Computing and Internet of Things (ICGCIoT). IEEE. https://doi.org/10.1109/ICGCIoT.2015.7380718

Tayyaba, S. K., Shah, M. A., Khan, O. A., & Ahmed, A. W. (2017). Software Defined Network (Sdn) Based Internet Of Things (Iot): A Road Ahead. 2017 International Conference On Future Networks And Distributed Systems, Icfnds 2017. https://doi.org/10.1145/3102304.3102319

Yavari, A., Panah, A. S., Schyndel, R. V., Georgakopoulos, D., & Jayaraman, P. P. (2017). Scalable Role-Based Data Disclosure Control For The Internet Of Things. Proceedings - International Conference On Distributed Computing Systems. 37TH IEEE International Conference On Distributed Computing Systems, ICDCS 2017 Atlanta, 2226-2233. https://doi.org/10.1109/ICDCS.2017.307