Bulletin of TUIT: Management and Communication Technologies

Volume 4 *2021-ikkinchi son* Article 4

April 2021

MODERN METHODS OF TESTING AND INFORMATION SECURITY PROBLEMS IN IoT

Halim Khujamatov

Ernazar Reypnazarov
Tashkent University of Information Technologies, reypnazar0vernazar@gmail.com

Amir Lazarev

Recommended Citation

Khujamatov, Halim; Reypnazarov, Ernazar; and Lazarev, Amir (2021) "MODERN METHODS OF TESTING AND INFORMATION SECURITY PROBLEMS IN IoT," *Bulletin of TUIT: Management and Communication Technologies*: Vol. 4 , Article 4.
Available at: https://uzjournals.edu.uz/tuitmct/vol4/iss2/4

UDC 004.7

MODERN METHODS OF TESTING AND INFORMATION SECURITY PROBLEMS IN IoT

Khujamatov H.E., Reypnazarov E.N., Lazarev A.P.

Abstract: This article analyzes the technology of the internet of things, ie its architecture, communication standards, threats to security and safety, methods and types of testing devices of the internet of things. In short, the architectures proposed by ITU-T and IWF, IEEE standards for Internet of Things, LPWAN standards, four levels of security (devices/gateways, network/transport, services and applications), components according to test methods, performance, loading, security, etc.

Keywords. Internet of Things, architecture, device, application, test methods, test types, communication standards.

Introduction

IoT (Internet of Things) is an entire ecosystem that includes intelligent sensors that provide remote control, storage, transmission and data security. IoT-reflect solutions in environmental, health, logistics and many more areas. It is necessary to solve problems with information security standards in IoT-devices, the architecture of connecting channels and devices. NIST, IEEE, ISO/IEC, which is now considered the largest organizations in the field of communication and information in the world, is trying to solve the above problems.

Recent scientific studies on data security in IoT devices show positive results, but these methods and approaches are based on traditional methods of network security. The development and application of security mechanisms for IoT devices is complex and not uniform. Therefore, the study of the security of IoT devices is one of the urgent tasks of today and is the purpose of this article.

With the above in mind, a number of tasks related to the security status of IoT devices have been identified and addressed:

- Analysis of existing standards and protocols for IoT;
- Study of security mechanisms for IoT devices;
- Analysis of methods for testing IoT devices.

The IoT infrastructure includes millions of interconnected objects and devices that exchange and store confidential information. For such IoT devices, theft and fraud scenarios such as hacking and falsification of personal data pose serious threats.

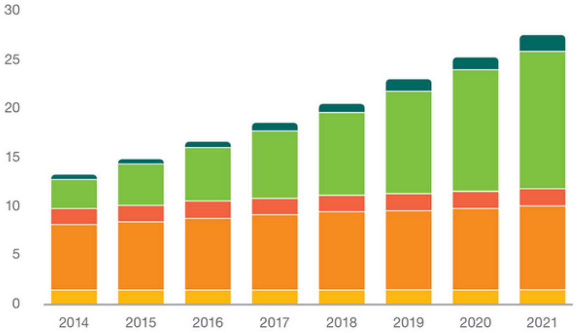


Figure 1. Growth dynamics of IoT devices, bln. per unit

In IoT, all smart devices are connected to each other via the Internet. The number of IoT devices and sensors was 21 billion in 2018, and is expected to exceed 50 billion in 2022 (Figure 1) [1], [2], [3], [4].

Given the above, IoT manufacturers are increasing the speed of production of smart devices, and at the same time, serious attention is not paid to the safety of devices

Main part

IoT architecture. Devices that are part of the IoT are any standalone devices, sensors and actuators that help remotely monitor and control.

The IoT ecosystem is the control panel, networks, gateways, analytics, data storage, security, and in general all the components that allow IoT users to connect their devices to each other [5], [6], [7].

To understand the existing solutions for the organization of IoT, you will need an architecture that describes the key components and their relationship. Figure 2 shows the benchmark architecture of IoT developed by the International Telecommunication Union (ITU-T) [8], [9].

The benchmark architecture of IoT developed by ITU-T includes the following.

Application layer - consists of all applications running on IoT devices.

The level of support for services and applications - provides the capabilities used in applications. Many take advantage of common features in the support of various applications. For example, shared capacity is used in data processing and database management [10], [11].

Special support capabilities are specific capabilities designed to meet the requirements of a specific set of IoT applications.

The network layer performs two main functions, i.e., the transport and network layer capabilities of the open systems interoperability benchmark model (OSI).

The level of control capabilities includes the traditional functions of network management, i.e. fault management, configuration management, computation management, performance management, and security management.

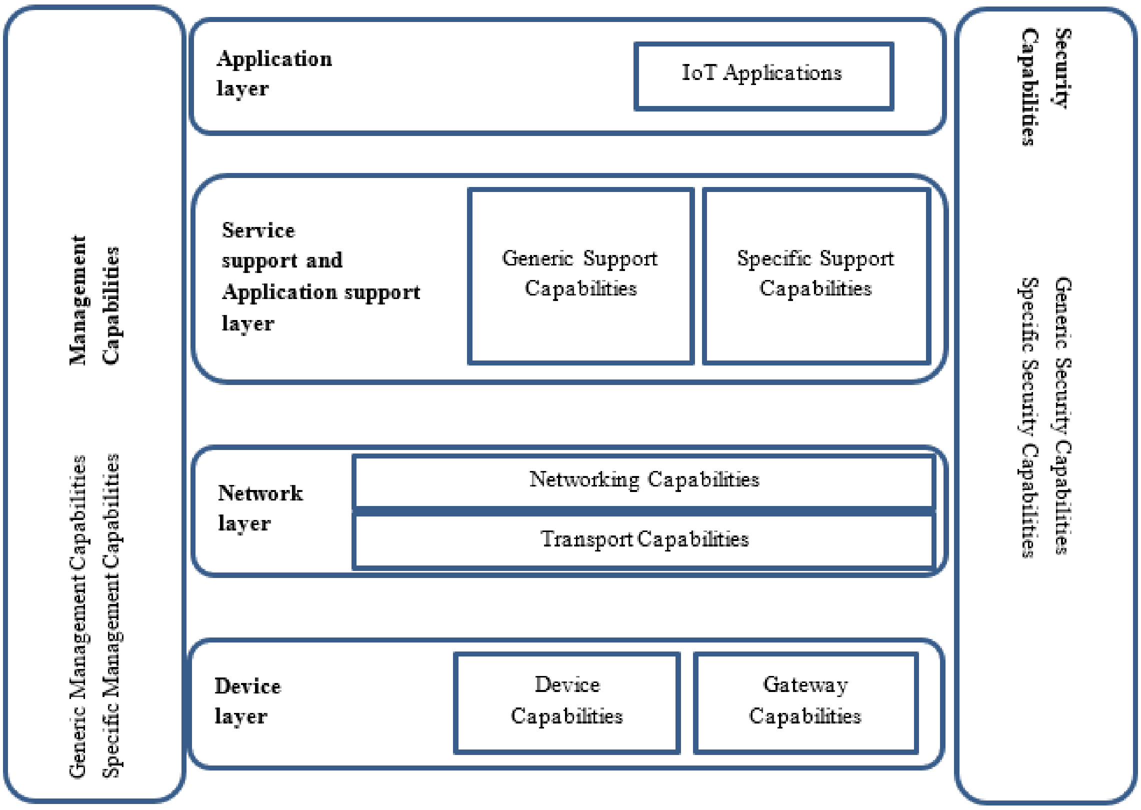

Management Capabilities
Generic Management Capabilities
Specific Management Capabilities
Application layer
IoT Applications
Service support and Application support layer
Generic Support Capabilities
Specific Support Capabilities
Network layer
Networking Capabilities
Transport Capabilities
Device layer
Device Capabilities
Gateway Capabilities
Security Capabilities
Generic Security Capabilities
Specific Security Capabilities

Figure 2. IoT benchmark architecture developed by the ITU-T

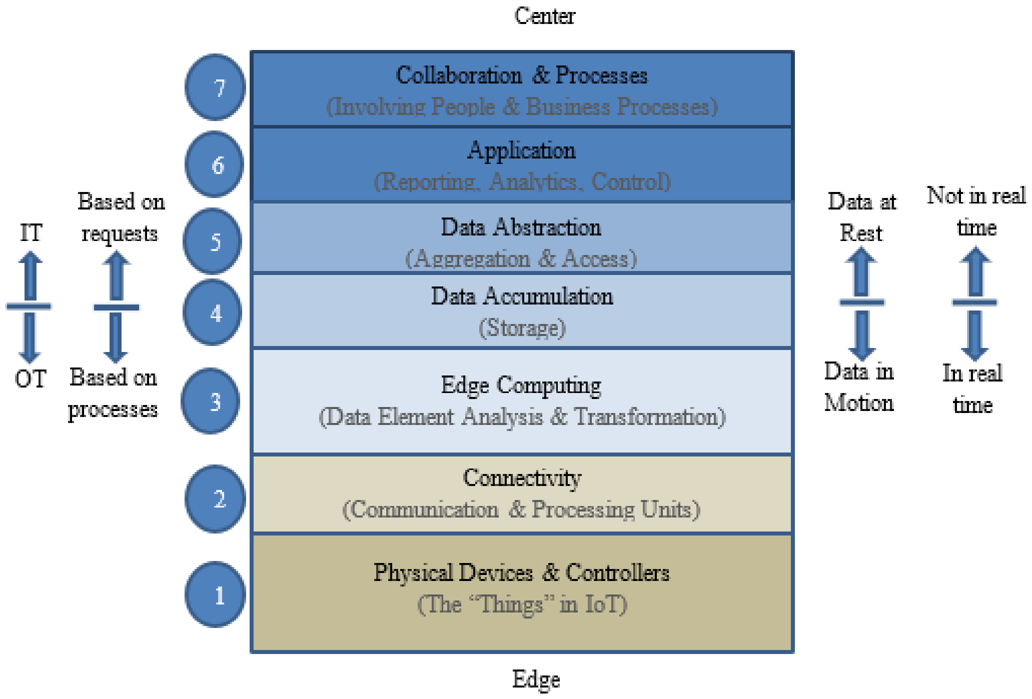
The level of security management capabilities includes the ability to provide general security independently of applications. Examples of general security in the Y.2060 description include:

• At the application level - authorization, authentication, protection of completeness and confidentiality of application data, protection of privacy, security audit and anti-virus protection;

• At the network level - authorization, authentication, confidentiality of use and signaling information, as well as protection of the completeness of signaling data;

• At the device level - authorization, authentication, device integrity checks, access control, data completeness and confidentiality protection.

The IoT World Forum (IWF) is also involved in the development of IoT architecture. It is an annual event attended by representatives of business, government and science. The option provided by them complements the ITU-T option because the IWF has focused on the high level that is important for the production of applications beyond the device and gateway level (Figure 3) [12].



Note: IT - information technology;
OT - operating technology.

Figure 3. IoT architecture developed by IWF.

The architecture developed by the IWF includes the following.

Level 1 is physical devices and controllers that can control multiple devices. This layer is almost identical to the device layer of the ITU-T architecture described above (Figure 2). These level elements are sensors and actuators. These devices can perform analog-to-digital and digital-to-analog conversions, data generation, and even support remote control.

Level 2 is similar to the network layer of the ITU-T architecture, except that the gateways are on the second level. Once the gateway is a network and communication device, it is preferable that it be at level 2.

Level 3. Processing at the level of peripheral computing is commonly referred to as fog computing. Fog computing is expected to be the distinguishing aspect of IoT. Unlike traditional cloud computing, cloud computing, data computing and resource storage in IoT are performed on peripheral devices.

At level 4, the peripheral computing level collects, processed and filtered data from different devices. It is then handed over to the higher levels for use.

At level 5, the peripheral adapts the data from different formats and from different processors coming from the computational level to use at higher levels.

Level 6 input includes various applications that use IoT data or manage IoT devices.

Level 7 has emerged as a result of the recognition that IoT is only beneficial if it interacts with people. This layer includes applications that share data and/or manage messages over the Internet, corporate network.

Creating an optimal security architecture for IoT devices will be needed primarily at a generalized platform, in manufacturing facilities or smart cities, and then at consumer levels. The security created should monitor all devices connected to the network separately, warn of unauthorized access, protect or disable devices when necessary. Therefore, the development and implementation of IoT standards is very important.

IoT standards. Active work on standardization is underway at all levels of IoT architecture. Today, large organizations such as the IEEE (Institute of Electrical and Electronics Engineers) and ISO/IEC (International Electrotechnical Commission) are engaged in the standardization of IoT technologies [13], [14].

In mid-2014, the first working group of IEEE P2413 began to develop the "Architectural Framework Standard for IoT", focusing mainly on the reliability and safety of devices.

In December 2015, an interagency working group on standardization of cyber security was established to coordinate issues in the field of cyber security at the international level [15].

Based on the above project, the National Institute of Standards and Technology (NIST) proposes to divide IoT into 5 functional areas [16]:

1. Connected devices;
2. IoT consumer class;
3. Medical devices and equipment used in the field of health care;
4. Smart buildings;
5. Smart production.

Standards should be developed taking into account the characteristics of these 5 industries.

Issues in the field of standardization for IoT have grown significantly, but ahead are the protection of personal data of IoT users, architecture, communication, etc. in-depth research in the areas.

The table 1 lists the IEEE's IoT-related standards [17], [18], [19].

Table 1.

IEEE standards for IoT

IEEE 802.15.4 ^{TM} -2011	IEEE standard for local and city networks i . 15 4 sections: a low-speed wireless personal networks (LR-WPAN)
IEEE 802.15.4 f ^{TM} -2012	IEEE standard for local and city networks i . 15 .4 Section: Low Speed Wireless Personal Networks (LR-WPANs). The system of active radio frequency identification (RFID) physical layer
IEEE 802.16 ^{TM} -2012	Air (wireless) interface l i IEEE standard for broadband wireless connection systems
IEEE 802.16 p ^{TM} -2012	Air (wireless) interface l i IEEE standard for broadband wireless connection systems . More: "Machine-to-machine applications, support for the improvement of the desired"
IEEE 1609.2 ^{TM} -2013	The IEEE standard for wireless access in the vehicle environment is security services for applications and management messages
IEEE 1703 ^{TM} -20 12	IEEE standard for LAN/WAN . Utilities industry o x Irgiz equipment data sheets as well as a node in the communication protocol
IEEE 1888 ^{TM} -2011	All Ubiquitous network management protocol for IEEE standard
IEEE 19 02.1 ^{TM} -2009	Flour foods protocols for the wavelength of the wireless network IEEE standard
IEEE 1905.1 ^{TM} -2013	IEEE standard for digital convergent home networks for heterogeneous technologies
IEEE 2200 ^{TM} -2012	IEEE standard for stream control on media client devices
IEEE 2030.5 ^{TM} -2013	The IEEE standard adopted for Smart Energy 2.0 i protocols
IEEE 21451-7 ^{TM} -2011	Smart Switching Interface for Sensors and Actuators - Transducers in Systems RFID Communication and Switch Protocols

Existing protocols of wired and wireless networks form an ecosystem of IoT devices. In IoT, wireless interrupt tolerance, data transmission efficiency, adaptability, scalability in low-speed conditions are important in providing wireless communication. There are several types of wireless to use for IoT [20], [21], [22]:

- Low Power Short Range Networks (LPSRN) are energy efficient networks with a small radius;
- Low Power Wide Area Networks (LPWAN) - energy efficient networks over a large radius;
- Cellular networks are a technology based on the use of cellular communications in a licensed range.Advantages of LPSRN:
- low costs of maintenance and implementation;
- authentication (in advanced versions);
- high density of devices (hundreds or thousands);
- energy efficiency of batteries (years).

It is irrelevant that the following advantage factors of the LPWAN communication protocol are balanced in meeting the requirements of different applications (smart home, smart city, smart power grid, smart car, etc.).

Advantages of LPWAN communication protocol:

- low demand for technical means;
- long-distance operation for sensors and small devices (15 km) and energy efficiency;
- low cost of service;
- Service life without battery replacement is 10 years or more.

Table 2 lists the LPWAN network standards that provide these advantages [23], [24], [25].

Table 2.

LPWAN network standards

LPWAN standard	Ingenu and RMPA	Link Labs and LoRaWan	LTE-M	Weightless and Nwave	UNB and SigFox	NB-Fi and WAVIoT
Frequency	2.4 Ghz	868 Mhz	1.8-2.7 Ghz	868 Mhz	868 Mhz	868 Mhz
Maximum distance	15000 m	10000 m	640 m	4000 m	10000 m	16600 m
The width of the node conduction k band	1 Mhz	125 kHz	192 kHz	200 Hz	100 Hz	100 Hz
Data en at work speed	2 kbit/s	0.3-50 Kbit/s	1 Mbit/s	100 bit/s	100 bit/s	10-100bit/s
Wireless update method	have	have	unknown	have	no	have
The operating mode of the gateway	half-duplex	half-duplex	duplex	transfer only	half-duplex	duplex
Number of devices in the gateway	500,000	40,000	20,000	50,000	50,000	1 mln. more than
Encryption	128 bit	128 bit	128-256 bit	not provided	128 bit	256 bit
Battery life	10 years	10 years	5 years	10 years	10 years	10 years
Time to market	2010	2014	2020	2013	2010	2011
Website	ingenu.com	link-labs.com	3gpp.org	mwave.io	sigfox.com	waviot.com

LPWAN technology is now widely used in building management, the implementation of the concept of “smart city”, asset tracking and many other processes.

IoT security. Security generally involves three features of information:

- usability;
- completeness;
- confidentiality.

Accessibility is a guarantee that users who have access to information will be able to use the information when they need it.

Completeness is a guarantee that only identified users will change the information.

Privacy is a guarantee that only users with access will be able to use the data.

Weaknesses in the issue of information security of IoT devices help many intruders gain access and confidential information.

In ensuring the safety of smart devices, the manufacturers of these devices must first and foremost take responsibility. At the same time, the most appropriate solutions should be made in accordance with the requirements and rules of information security. In most cases, manufacturers of IoT devices do not pay attention to the application of safety measures in the development of their products.

Many IoT solutions consist of basically four levels. At each of these four levels, IoT-solution components must have appropriate protection against various vulnerabilities. That is:

1. Device/gateway level: should be protected from fraudsters who send malicious commands or from hackers who try to listen to the confidential information of sensors transmitted from the devices.
2. Network/transport layer: it is necessary to protect the device from sending fraudulent measurements, which can damage the data stored in the applications.
3. Level of support for services and applications: the database and control commands should be protected from various remote control attacks.
4. Application level: Analytical processes performed at the application level should be protected from manipulation or data misuse.

IoT security threats. Security threats in IoT can be implemented in the following sections of the network:

1. Wireless data transmission systems;
2. Base station;
3. Network management and application servers;

Wireless data transmission systems. Wireless data transmission systems are likely to face the following threats:

- creation of artificial noise in order to reduce the signal quality;
- capture and modify transmitted data.

There are two ways to reduce the likelihood of these threats:

- Organization of wireless transmission in accordance with the requirements;
- Use of data encryption and device authentication tools.

Base station. Threats in this section can only be considered when building autonomous base stations, i.e. when the IoT network is independent of providers. If the provider's services are used, the responsibility for addressing the threats remains with the provider. Threats to the base station include:

- Violation of the base station control console;
- Theft of access rights by introducing malware into the base station;
- DDoS attacks;
- Power outage;
- Device theft.

In this case, the first thing to do is not to connect the base stations directly to the Internet. Depending on the technical capabilities, it is preferable to use the networks of other providers. Again, the operating system of the base station will need to be configured accordingly, and the following is recommended:

- use of secure remote control protocols;
- placement of base station management interfaces in separate network segments to be checked;
- delete unused protocols and functions;
- ensure backup of settings;
- uninterruptible power supply of the base station.

Network management and application servers. This section is the most complex section on IoT security. Because servers are a major part of IoT. They control the connection of base stations and devices, receive and decode data from sensors, and transmit that data to higher levels for use in the management and calculation of technological processes. In addition, the application server can store old data about the operation of the IoT network. Ordinary servers are more vulnerable to all of today's threats than the specialized devices discussed above, which are [26]:

- viruses;
- zero-day attacks;
- interception of data in the interval;
- DDoS attacks;
- Violation of settings as a result of uncoordinated actions of service providers;
- data loss without reservation.

In general, the number of threats in this section is very high and they are well known. The security tools used in the department can be divided into two classes:

- Built-in security mechanisms;
- External means of protection.

The built-in security mechanisms are the settings of the operating system and the software used.

External protection tools include antivirus, integrity check, firewalls, intrusion detection and prevention systems, backup systems, security scanners.

Given the specificity of IoT, the following next-generation protection tools can also be used: Web Application Firewall, Endpoint Detection and Response (EDR), Network Forensics (NF), Threat Intelligence (TI), Security Operation Center (SOC) [27].

Each component of the IoT infrastructure can be a primary target or a key element of a threat. Therefore, it is necessary to provide comprehensive security.

Modern methods of IoT testing. The number of IoT devices is increasing day by day and this is creating new technical and technological opportunities in various fields. However, there are also cases where they fail in simple scenarios devised by their creators. Therefore, a number of issues arise on how to test IoT devices [28], [29].

Methods of testing IoT. When testing IoT devices, more attention is paid to checking their network interconnection, security, and device performance. Testing IoT goes beyond the boundaries of devices and sensors because IoT involves large volumes and a variety of generated data that create additional challenges. In addition, there is currently no single approach designed to test IoT.

There are currently four main areas of testing for IoT devices. These directions should be taken into account in the production of all IoT products that have access to the Internet. The directions for IoT testing are shown in Figure 4.

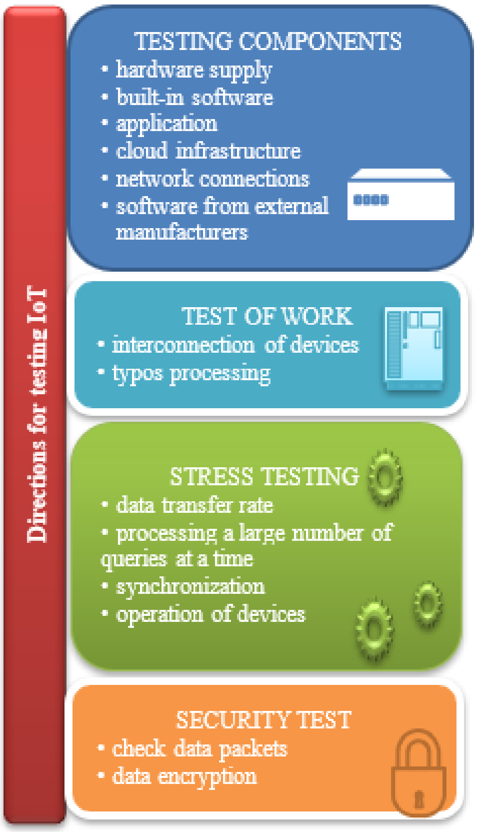


Figure 4. Four main areas of testing IoT devices.

In addition to testing physical devices, there are also ways to test virtual tools. Virtual tools can be stored, processed and used. Software is an example of such a tool.

The most common ways to test software:

1. Modular test. In this method, the software components are checked separately in order to identify possible errors. This re-

quires a good knowledge of the program content, and this is usually done by programmers.

2. Integration test. Basically detects interface errors. During the module test, the tested software components are integrated with each other and checked for problems.

3. Systematic testing. At this stage, all operating conditions of the overall system are analyzed, with hardware and software organizers interrelated.

4. Try the "black box" method. To develop effective test methods, it is necessary to know the architecture of the device, the type of operating system, the interconnection protocols without knowing the internal mechanisms of the test object Figure 5 [30], [31], [32].

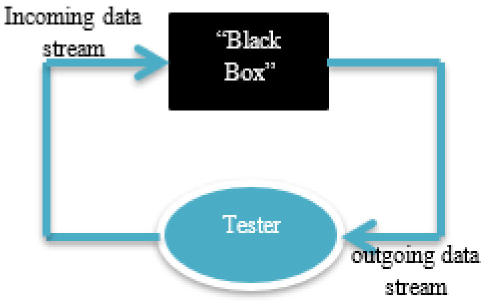


Figure 5. "Black box"method.

The software is also used appropriately on IoT devices. The process of testing them is as important as the process of physical devices.

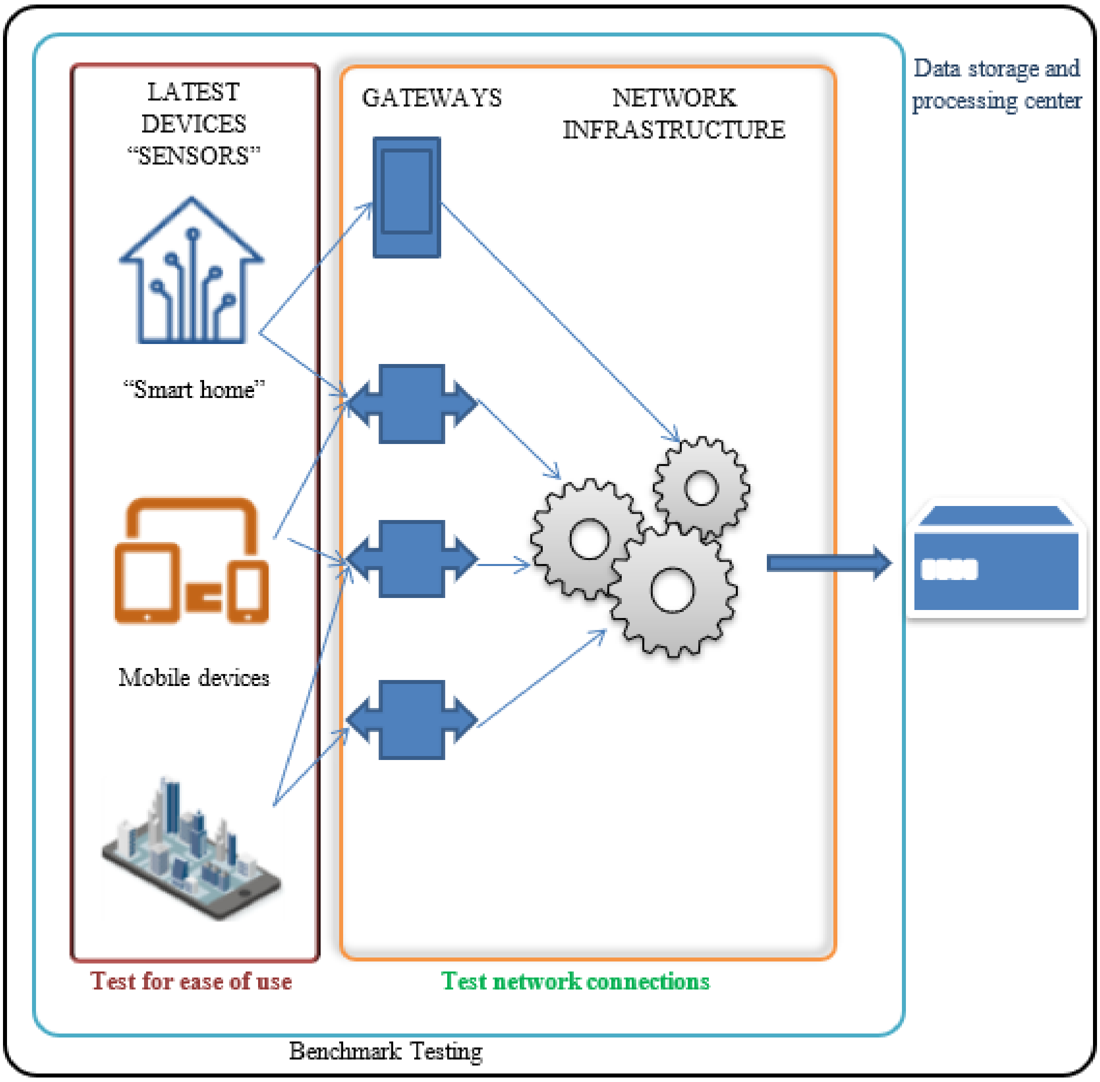


Figure 6. Types of IoT testing.

Types of IoT testing. In this section, we consider some types of testing performed by testers to ensure that IoT systems work in the same order (Figure 6).

Usability Testing. The capabilities of IoT should meet the requirements of the user. The user should have no problem knowing the capabilities of the product they are using. The use of this test method focuses on ease of learning. To conduct such a test, it is necessary to gather a group of users who meet certain criteria. The result is to help improve product quality through evaluations during subsequent production [33], [34].

Connectivity Testing. IoT-elements should work in conjunction with each other. Therefore, attention should also be paid to the different connection methods and the exchange of information between the user and the device. When testing network connections, the environment in which the device is used (network type, signal strength, weather conditions, etc.) is taken into account and its operation is checked according to the conditions included in it [35], [36].

Benchmark Testing. The main task of such a test is to take into account the problems that lead to network outages. Testers should comprehensively analyze how quickly the data travels from one node to another.

Security Testing. There are two main types of security testing:

1. Static test. This is done manually or using code verification tools. The main task is to analyze the code of the program written for the device and identify possible security problems.

2. Dynamic testing. This is done using special tools, i.e. authentication problems, simulation of attacks, unauthorized use of device memory, etc. checked.

Testing processes are very necessary. Therefore, it is necessary to use special simulators that mimic the operation of IoT-devices and network nodes, which in turn will help the devices to reduce costs and optimize the organization of networks.

Conclusion

This article discusses the development of IoT technology, architectures, standards, security, security threats, test directions and methods. The performance of IoT generally depends on network technologies, as the data generated on the devices must be transmitted and processed to the desired addresses. Security must also be taken into account in the transmission process.

Given the above, it can be predicted that a lot of work will be done on IoT technology instead of the conclusion.

References

[1]Internet veshey, IoT, M2M mirovoy rinok http://www.tadviser.ru/index.php/Statya:Internet_veщshy,_IoT,_M2M_(mirovoy_rinok)

[2]Khujamatov Kh.E. Khasanov D.T., Reypnazarov E.N. Modeling and Research of Automatic Sun Tracking System on the bases of IoT and Arduino UNO // International Conference on Information Science and Communications Technologies ICISCT 2019, Tashkent, Uzbekistan - 2019. DOI: 10.1109/ICISCT47635.2019.9011913

[3]Davronbekov D.A., Aliev U.T., Isroilov J.D., Alimdjanov X.F. Power Providing Methods for Wireless Sensors // 2019 International Conference on Information Science and Communications Technologies. Applications, Trends and Opportunities, ICISCT 2019. - p.1-3

[4]Siddikov I.Kh., Sattarov Kh.A., Khujamatov Kh.E. Modeling of the Transformation Elements of Power Sources Control // International Conference on Information Science and Communications Technologies (ICISCT) Applications, Trends and Opportunities, 2nd, 3rd and 4th of November 2017, Tashkent, Uzbekistan. DOI: 10.1109/ICISCT.2017.8188581

[5]IoT ecosystem https:// www.intel.ru/content/www/ru/ru/internet-of -things/ecosystem.html

[6]Davronbekov D.A., Muxamedaminov A.O., Axmedov B.I. The Role of Wireless Networking Technology Today // "Innovatsionnie nauchnie issledovaniya: Teoriya, Metodologiya, Praktika". Sbornik statey XX Mejdunarodnoy nauchno-prakticheskoy konferensii, 2020. - p. 77-79

[7]Siddikov I.Kh., Sattarov Kh.A., Khujamatov Kh.E., Dekhkonov O.R. Modeling the processes in magnetic circuits of

electromagnetic transdusers // International Conference on Information Science and Communications Technologies ICISCT 2016, 2nd, 3rd and 4th of November 2016, Tashkent, Uzbekistan. DOI: 10.1109/ICISCT.2016.7777393

[8]Recomendation of ITU-T Y.2060 for Internet of Things (IoT) https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11559&lang=ru

[9]Khujamatov Kh.E. Khasanov D.T., Reypnazarov E.N. Research and Modelling Adaptive Management of Hybrid Power Supply Systems for Object Telecommunications based on IoT // International Conference on Information Science and Communications Technologies ICISCT 2019, Tashkent, Uzbekistan - 2019. DOI: 10.1109/ICISCT47635.2019.9011831

[10] Muradova A.A. Khujamatov Kh.E. Results of Calculations of Parameters of Reliability of Restored Devices of the Multiservice Communication Network // International Conference on Information Science and Communications Technologies ICISCT 2019, Tashkent, Uzbekistan - 2019. DOI: 10.1109/ICISCT47635.2019.9011932

[11] Khujamatov H., Reypnazarov E., Akhmedov N., Khasanov D. IoT based Centralized Double Stage Education // 2020 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan – 2020. DOI: 10.1109/ICISCT50599.2020.9351410

[12] Recomendation of IWF for Internet of Things (IoT) https://www.iotwf.com/

[13] IEEE Internet of Things https://iot.ieee.org/ (date of appeal 18.02.21)

[14] International Electrotechnical Commission https://www.iec.ch/ (дата обращения 21.01.21)

[15] Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT) https://csrc.nist.gov/publications/detail/nistir/ 8200/draft

[16] NIST: Internet of Things https://www.nist.gov/topics/internet-things-iot

[17] IEEE Standard for Local and metropolitan area networks--Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) http://standards.ieee.org/findstds/standard/802.15.4-2011.html

[18] Davronbekov D.A., Rakhimov B.N., Alimdjanov X.F., Axmedov B.I. Review of Wearable Wireless Sensor Network // Scientific Collection «InterConf», (41): Proceedings of the 7th International Scientific and Practical Conference «Scientific Horizon in The Context of Social Crises», February 6-8, 2021, Tokyo, Japan: Otsuki Press, 2021.- p.1052-1058

[19] Khujamatov Kh., Ahmad Kh., Reypnazarov E., Khasanov D.. Markov Chain Based Modeling Bandwith States of the Wireless Sensor Networks of Monitoring System//International Journal of Advanced Science and Technology, Vol. 29, No.4, (2020), pp. 4889 – 4903. http://sersc.org/journals/index.php/IJAST/article/view/24920

[20] Siddikov I.Kh., Sattarov Kh.A., Khujamatov Kh.E. Modeling and research circuits of intelligent sensors and measurement systems with distributed parameters and values// "Chemical technology control and management" International scientific and technical journal, Tashkent 4-5/2018/ pp. 50-55.

[21] Siddikov I.Kh., Khujamatov Kh.E., Khasanov D.T., Reypnazarov E.R.. Modeling of monitoring systems of solar power stations for telecommunication facilities based on wireless nets// "Chemical technology. Control and management" International scientific and technical journal, 2020, №3 (93) pp.20-8. https://uzjournals.edu.uz/ijctcm/vol2020/iss3/4

[22] Davronbekov D.A., Matyokubov U.K. The Role of Network Components in Improving the Reliability and Survivability of Mobile Communication Networks // Acta of Turin Polytechnic University in Tashkent. 2020, Vol.10: Iss.3, Article 2. - p.7-14

[23] Morin E., Maman M., Guizzetti R., Duda A. “Comparison of the device lifetime in wireless networks for the internet of things,” IEEE Access, vol. 5, pp. 7097–7114, 2017

[24] Khujamatov H., Reypnazarov E., Hasanov D., Nurullaev E., Sobirov Sh. Evaluation of characteristics of wireless sensor networks with analytical modeling // Bulletin of TUIT: Management and Communication Technologies Bulletin of TUIT: Management and Communication Technologies, Volume 3, December 2020. https://uzjournals.edu.uz/tuitmct/vol4/iss1/4

[25] Khujamatov H., Toshtemirov T. Wireless sensor networks based Agriculture 4.0: challenges and apportions // 2020 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan – 2020. DOI: 10.1109/ICISCT50599.2020.9351411

[26] Bernard Schulz “Kontrolno-izmeritelnie resheniya dlya programmno-opredelyaemix radiosistem (SDR)”, “Rohde&Schwarz”, 2012 – 1MA206 1e

[27] Kikilo Sergey “Opasnosti i zaщita IoT-kommunikatsiy”, Connect WIT 2019 №7-8

[28] Khujamatov H., Khasanov D., Reypnazarov E., Akhmedov N. Industry Digitalization Consepts with 5G-based IoT // 2020 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan – 2020. DOI: 10.1109/ICISCT50599.2020.9351468

[29] Davronbekov D.A., Isroilov J.D., Alimdjanov X.F., Norkobilov S.A., Axmedov B.I. Analysis of Features of Wireless Sensor Networks // Scientific Collection “InterConf”: Proceedings of the 7th International Scientific and Practical Conference “Scientific Horizon in The Context of Social Crises”, February 6-8, 2021, Tokyo, Japan: Otsuki Press, 2021.-p.1044-1051

[30] Dolgushev R.A., Kirichek R.V., Kucheryaviy A. Ye. “Obzor vozmojnix vidov i metodov testirovaniya internet veshey” Informatsionnie texnologii i telekommunikatsii. 2016. T. 4. No 2.

[31] Khujamatov Kh., Khasanov D., Reypnazarov E., Akhmedov N. Networking and Computing in Internet of Things and Cyber-Physical Systems // The 14th IEEE International Conference Application of Information and Communication Technologies, 07-09 October 2020, Tashkent, Uzbekistan. DOI: 10.1109/AICT50176.2020.9368793

[32] Khujamatov H., Reypnazarov E., Akhmedov N., Khasanov D. Blockchain for 5G Healthcare architecture // 2020 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan – 2020. DOI: 10.1109/ICISCT50599.2020.9351398

[33] Davronbekov D., Aliev U.T., Isroilov J.D. Using the energy of electromagnetic radiation as a source of power // 2017 International Conference on Information Science and Communications Technologies, ICISCT 2017

[34] Siddikov I.Kh. Sattarov Kh.A. Khujamatov Kh.E. Dexkhonov O.R. Agzamova M.R. Modeling of Magnet Circuits of Electromagnetic Transducers of the Three-Phases Current//2018 XIV International Scientific-Technical Conference on Actual Problems of Electronics Instrument Engineering (APEIE-2018), October 2-6, 2018, Novosibirsk. –p.p. 419-422. DOI: 10.1109/APEIE.2018.8545714

[35] Kirichek R., Koucheryavy A. Internet of Things Laboratory Test Bed // Lecture Notes in Electrical Engineering. 2016. Vol. 348. PP. 485–494.

[36] Arsheen S., Wahid A., Ahmad Kh., Khujamatov Kh. Flying Ad hoc Network Expedited by DTN Scenario: Reliable and Cost-effective MAC Protocols Perspective // The 14th IEEE International Conference Application of Information and Communication Technologies, 07-09 October 2020, Tashkent, Uzbekistan. DOI: 10.1109/AICT50176.2020.9368575