

New Security Challenges of Internet of Things

Gennady Dik[1,3(✉)], Alexander Bogdanov[1,2], Nadezhda Shchegoleva[1,2], Jasur Kiyamov[1], and Aleksandr Dik[1]

[1] St. Petersburg University, Saint Petersburg, Russia
{a.v.bogdanov,n.shchegoleva,z.kiyamov,a.dik}@spbu.ru
[2] St. Petersburg State Marine Technical University, Saint Petersburg, Russia
[3] St. Petersburg LLC "System Technologies", Saint Petersburg, Russia
g.dick@systechnologies.ru

Abstract. The paper addresses current security issues of the Internet of Things (IoT), analyzes the most recent and significant violations in this area, proposes a variant of an integrated approach both to protecting the IoT devices themselves and to promising methods organization of interaction using 5G (6G) networks. Particular attention is paid to the process of threat modeling in assessing IoT security, as well as the application of machine learning (ML) principles in order to ensure the protection of the infrastructure of the Internet of things. Practical recommendations are given for organizing measures to improve the security of promising IoT networks.

Keywords: IoT · Smart Habitat · IT-System · 5G · 6G

1 Introduction

In the modern world, IoT devices are not only computers and TVs, tablets and smartphones, smart watches and kitchen appliances, etc. Almost all electronic devices involved in our daily lives can potentially be connected to a single computer network and become part of the Internet of things. The information circulating in this network contains huge amounts of not only information about its owners, but also data of varying degrees of confidentiality, including control signals, status messages, etc. All this data can be either stolen by intruders or distorted for criminal purposes, and IoT devices can be hacked or turned into a non-working "brick". As a result, an increase in the number of IoT devices produced and connected inevitably leads to an increase in the ability of cybercriminals to violate IT security, including the security of the Internet of Things [1].

2 Relevance of IoT Security Threats

The security breach of the Internet of Things can eventually have quite serious and sometimes catastrophic consequences. Attackers can hack and then gain

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2023
O. Gervasi et al. (Eds.): ICCSA 2023 Workshops, LNCS 14109, pp. 302–316, 2023.
https://doi.org/10.1007/978-3-031-37120-2_20

access to a drone or any vehicle controlled via IoT, reconfigure their functionality, security system, etc. Hacking the IoT devices of Smart Homes, Smart Cities and Smart Habitats (SH) will allow cybercriminals to control people's living environment. In medicine and healthcare, in financial institutions (banks) and telephone companies, the access of intruders to the Internet things used in these areas will lead to the disclosure and dissemination of personal (confidential) information about the patient, client, subscriber. In addition, disruption of the functioning of medical devices, banking equipment and equipment of telephone operators leads not only to a deterioration in the quality of life, but also to serious threats to its existence. Cyber attacks on industrial or military Internet of Things systems can lead to a number of irreversible destructive consequences (Fig. 1).

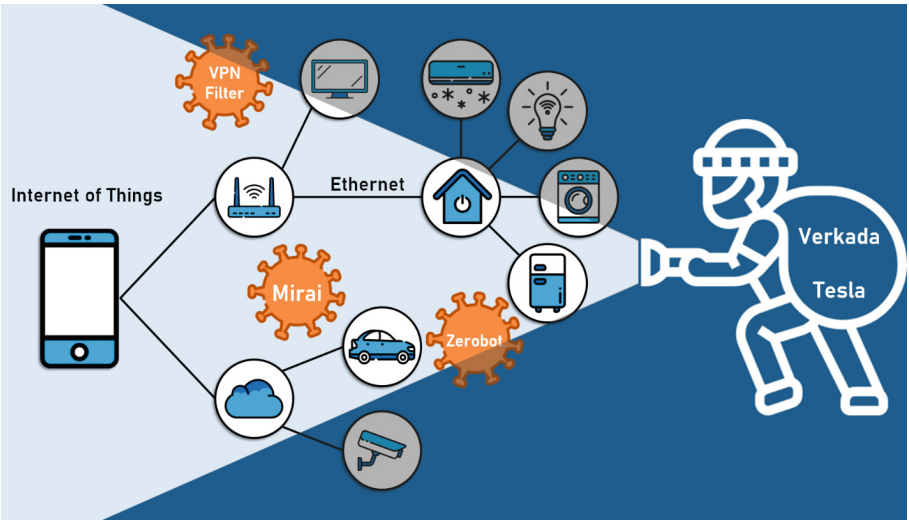

Fig. 1. IoT security breaches

According to a study by Kaspersky Lab JSC, in recent years there have been a number of high-profile cases of compromise of Internet of Things devices by cybercriminals, namely [2]:

- 2016 - Mirai botnet attack, when hundreds of thousands of compromised pluggable devices were involved in the botnet to perform malicious activities such as registration, emulation of "interested client" actions, password theft, and more. The Mirai botnet attack disrupted major services and websites such as Spotify, Netflix and PayPal.
- 2018 - VPNFilter malware infects about half a million routers in more than 50 countries, while VPNFilter malware can be installed on devices connected to the router, and then using malware, collect passing information, block network traffic and steal passwords.

- 2020 - Tesla Model X hack, when a cybersecurity expert hacked a Tesla Model X car in less than two minutes using a Bluetooth vulnerability, which, according to experts, applies to other car models using wireless access.
- 2021 - Verkada video camera hack (Verkada is a surveillance camera company), when Swiss hackers gained access to 150,000 live feeds including cameras at Tesla factories and warehouses, Cloudflare offices, Equinox gyms, hospitals, prisons, schools, police stations and Verkada's own offices.
- 2022 - the attack of the Zerobot botnet, which spreads through the exploitation of almost two dozen vulnerabilities in IoT devices and various software (including F5 BIG-IP, Zyxel firewalls, Totolink and D-Link routers, and Hikvision cameras) [3].

The above list of attacks by intruders on IoT (and this is a very small selective part) clearly demonstrates the seriousness of the possible consequences for all spheres of life in the modern world.

Thus, this is not only a matter of IT security, it is a matter of ensuring the security of all aspects of the life of modern society. To understand it, it is necessary to consider the basic principles of building the Internet of things.

3 Purpose and Basic Principles of Building the Internet of Things

In public opinion there is no exact generally accepted definition for the term "Internet of Things" [4]. At the same time, according to the recommendation of the International Electronics Union (ITU), IoT is understood as a global infrastructure for the information society, which enables the provision of more complex services by connecting (physical and virtual) things to each other based on existing and developing interoperable information and communication technologies (ICT) [5].

Thus, the Internet of Things is a network of things, where the word "things" refers to intelligent objects that have embedded electronics, sensors and embedded technologies for interacting with the external environment with the ability to transmit data about their current state and receive data from outside [5]. To implement their functionality, these "things" are equipped with general software (software), which includes an operating system and other general-purpose software tools that are not focused on solving problems of any particular subject area. They also have special software (SW) installed on them, which includes programs that implement the selected functions of the system, and is developed on the basis of common software. The article deals with the issue of using open source software, since general software is usually standardized and universal. Expanding the capabilities of IoT devices allows us to define the "Internet of Things" as a computer network of physical objects equipped with built-in technologies for collecting and transmitting information in conjunction with devices and technologies for storing and intelligently processing information, as well as devices and algorithms for generating control actions on parts or the entire system generally.

The theory and practice of using the Internet of things shows that their main purpose is to improve the quality of life of the population, to make the process of people's life more dynamic and convenient. These circumstances eventually led to an explosive growth in the use of IoT devices. According to Cisco analysts, by the end of 2023, on average, each person in Russia will have more than six connected devices operating online (for example, a computer, mobile phone, smartphone, phablet and tablet, a smart home control device, a device for monitoring health indicators, etc.) [6,7].

For the full functionality of IoT, it is necessary to first define (identify) the object, and then involve it in an ever-expanding circle of network connections. The Internet of Things is inherently a continuous flow of data in space, passing through different networks around, which leads to the emergence of the so-called "web of things". The functioning of this "web" is possible under the following two conditions [8]:

1. mandatory identification of each specific object from the IoT;
2. continuous switching of the growing volume of information and objects in the network, which, in turn, will also be combined in the network.

At the same time, the implementation of IoT technology is carried out by the following functional components (ABCDE-components) [9] (Fig. 2):

1. **Analytics** – is designed to analyze information coming from data collection devices (sensors, controllers, video cameras, etc.). Based on the processing results, control signals are generated for IoT devices. Analytical platforms (SSW modules), depending on the complexity of information processing and its volume, can be installed locally, in the cloud, or have a hybrid version of their placement.
2. **Big Data** – in this context, it is a distributed database designed to organize the storage of all primary (raw) and processed information on the involved IoT [10].
3. **Connection** is a combination of ICT options necessary for the functioning (all kinds of wired and wireless networks, various physical methods of connecting IoT devices, SPD protocols, switching devices, routing, signal amplification, etc., as well as switching open source software).
4. **Devices** – this is a set of devices designed for retrieving information, displaying it, issuing a control action, etc.
5. **Experience** – in the context of application for the Internet of things, it is considered as an option for using knowledge to build and improve IoT devices based on the accumulated "baggage" and further moving forward.

Based on the presented principles of functioning of the technology of the Internet of things (according to the designated functions and component construction), it is possible to determine the basic components of the IoT and the main ways to combine them into a single "web" or data transmission system (DTS). Then it is advisable to include the following main elements in the infrastructure construction of the Internet of Things (Fig. 3):

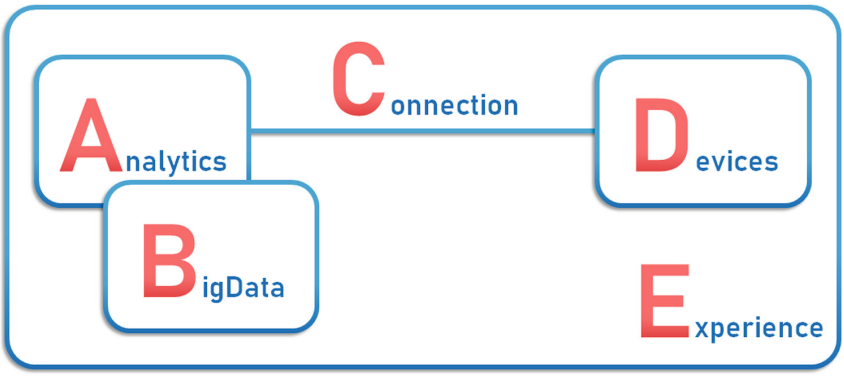

Fig. 2. Components of the implementation of the technology of the IoT

1. IoT devices - various types of sensors and various electronic devices connected to the DTS [11,12].
2. Information storage and processing systems - computer systems for collecting, processing, generating recommendations, reports, control actions, etc. [13].
3. Communication systems - wired and wireless networks, including equipment for their operation [8,14,15].
4. SSW - software designed to ensure the performance of IoT [16].

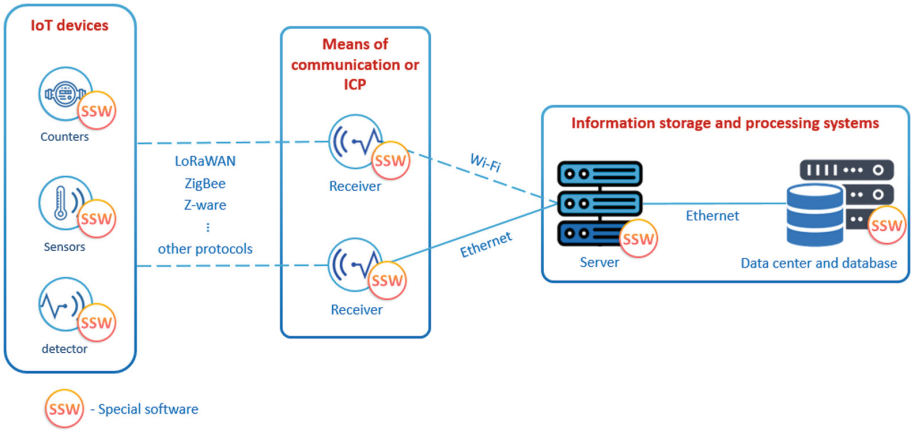

Fig. 3. IoT infrastructure

At the same time, possible integrations and combinations of the above-defined basic elements of the Internet of things should be taken into account (for example, modern video cameras may contain SSW for analytics and critical situations

recognition and independently generate alarm signals and control actions). But it is precisely these basic elements of the IoT infrastructure that represent a "tasty" world of opportunities for attackers (hackers, cybercriminals) [17,18]. For this reason, further in the article, an analysis of possible security problems and existing IoT threats will be given in order to subsequently determine a set of measures to protect the Internet of Things.

4 Problem Analysis of Internet of Things Security Issues

Consideration of IoT security issues starts with the model of the Internet of Things. In accordance with the previously defined infrastructure for the interaction of smart things, a variant of the IoT reference model is presented in Fig. 4. This model contains four infrastructure layers:

- application layer;
- service support and application support layer;
- network layer;
- the level of IoT devices.

The process of functioning of the proposed levels provides managerial impacts, and the process of ensuring the security of the Internet of things: general in software and hardware.

The overall security of the Internet of things is aimed at solving current administrative, legal and other issues, that decrease in the security of IoT:

1. Lack of legislative acts, norms, as well as uniform standards, rules and instructions for IoT.
2. Saving of manufacturers on safety in the development and further implementation (release for sale) of smart things [19].
3. Lack of clearly defined physical or legal liability in the operation of the Internet of things [20].
4. The presence of "staff shortage" or a significant lack of experienced specialists in the field of IoT [21].
5. Dissemination (unintentional) of confidential information by users or maintenance personnel during operation, as well as employees during the creation of IoT.

There are known cases of publication in wide circles of technical information about IoT devices that have not yet switched to service. Employees fired or moving to other companies often become a source of "secrets".

As for the software and technical issues of ensuring the security of the Internet of things, they should include:

1. Compliance with security requirements at the stages of development, testing and implementation (release for sale) of software and hardware of IoT devices.

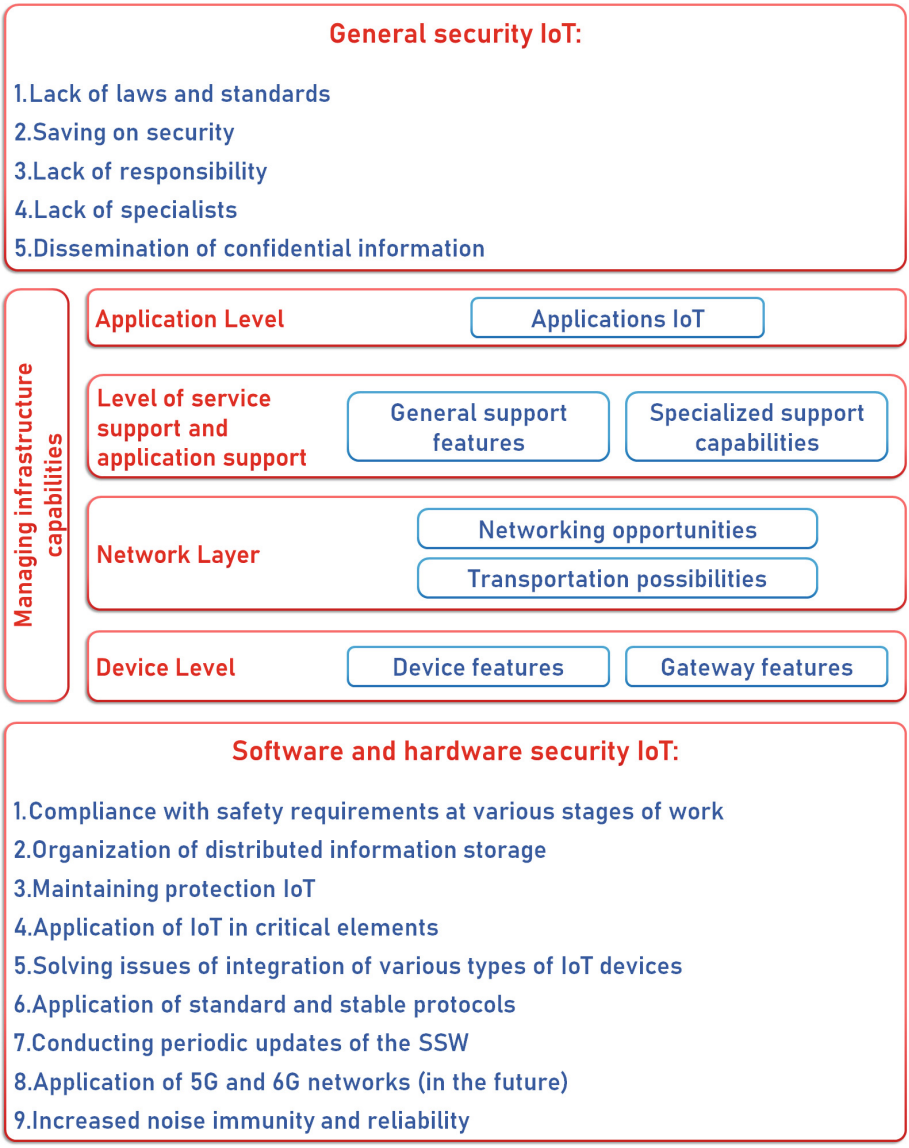

Fig. 4. Variant of the IoT Reference Model

2. Organization of distributed cloud, edge and hybrid storage of information on virtual machines for various IoT service providers so that data is not inaccessible or completely lost for everyone in the event of an attack by intruders on one service provider or IoT device.

3. Maintaining the protection of the Internet of Things in the face of an ever-expanding area of attacks on smart things, taking into account the improvement in the methods and speed of attacks on the IoT infrastructure.
4. Fulfillment of security requirements when using IoT in critical infrastructure elements of the industrial Internet of things (IIoT), in military systems (Battle IoT or BIoT), etc.
5. Compliance with security requirements when solving the issues of integration of various types of IoT devices, taking into account the complexity of the infrastructure construction and the diversity of the Internet of things.
6. The use of standard and stable developments in the construction of ICT, to exclude the use of both proprietary or less well-known protocols that do not meet security standards, and various methods of connecting devices through "crutches", etc.
7. Periodic updating of SSW, IoT "firmware" and ICT equipment (outdated software may contain not only errors and "security holes", but also has a high probability of being hacked by cybercriminals).
8. Improving the noise immunity and reliability of software and hardware in order to counter planned actions by intruders (crashes, failures, etc.).
9. Building ICT based on 5G networks, as well as working out the issue of using 6G networks as options for promising means of communication (hereinafter, the 5G communication standard is mainly considered).

Moreover, taking into account the peculiarities of the architecture and landscape of 5G (6G) networks, which include a large number of connections and high bandwidth, serious consequences of failures and abuses (cloud technology and a variety of services) and placement of equipment outside the protected circuit, it is necessary to plan the organization of protection at three levels [9]:

- The first level is protection at the level of implementing technical solutions, building network infrastructure and equipment placement options:
  - use of a powerful firewall between users and the outside world, multi-level isolation and integrity protection of SDN (Software-defined Networking) and VNF (Network Functions Virtualization) components - hypervisor, virtual machines, OS, controllers and containers;
  - application authentication in Mobile Edge Computing (MEC), use of an additional authentication factor when accessing the corporate network, whitelisting of devices and services, authorization of requests in the application programming interface (API);
  - ensuring high availability of virtual machines for fast recovery after attacks;
  - trusted hardware environment – safe booting of devices, application of TEE (Trusted Execution Environment) technology;
  - real-time attack detection on network nodes and virtual infrastructure elements using artificial intelligence algorithms.
- The second level is protection at the level of network infrastructure management:

  - secure management of not only user data, but service, technical, analytical and other types of information involved in ensuring the functioning of the Internet of things (the so-called attack on the subscriber and attack on the mobile operator), using encryption, anonymization, depersonalization and etc.;
  - centralized management of identified vulnerabilities, as well as policies and levels of information security, use of information in the course of ongoing analysis of big data to detect anomalies and promptly respond to attacks;
  - comprehensive use of counterfeit base station detection tools based on real-time monitoring of operational and maintenance events;
  - application of multi-factor authentication algorithms and organization of access differentiation to segments by O&M (Operations & Maintenance or Operation and Maintenance).
- Third level - protection at the level of the standard:
  - separation of the layers of the data transmission and reception protocol into three planes: User Plane, Control Plane, Management Plane. With complete isolation, encryption (of subscriber and signal traffic), and control of the integrity of these planes;
  - use of encryption methods for subscriber and technological traffic with an increase in the length of the encryption key up to 256 bits;
  - application of a unified subscriber authentication mechanism for various types of wireless communications;
  - support for flexible security policies for segments;
  - use of unified standards, etc. [9].

The implementation of the presented set of measures is a rather complicated and time-consuming task. This article proposes to consider the use of machine learning methods, which, as you know, can do what humans cannot, providing automation for large-scale analysis of possible threats and ways to protect. Thanks to ML, it is planned to solve a growing number of problems in the field of cybersecurity: scaling security solutions, detection of unknown attacks and detection of complex attacks, including polymorphic malware and other tasks [22]. When applying machine learning methods in the tasks of ensuring the protection of the Internet of Things infrastructure, it is proposed to carry out threat modeling in order to assess IoT security (according to one of the threat classification models).

5 Ways to Model IoT Threats

It should be noted that in the course of threat modeling, it is possible not only to identify attacks on IoT devices and rank risks according to their severity, but also to consider options for using machine learning methods to ensure the security of Internet of things. To do this, it is proposed to apply a software-oriented approach that targets the vulnerabilities of each application component, based

on the STRIDE threat classification model [18], which focuses on identifying weaknesses in software and hardware, rather than modeling vulnerable Internet of Things assets, risk assessment (DREAD) or analyzing the behavior of likely attackers [23].

The STRIDE threat classification model, developed by Prairite Garg and Lauren Confelder (Microsoft), is one of the most popular threat classification systems [24]. The abbreviation STRIDE stands for the following types of threats:

1. Spoofing - bypassing the access control system by disguising it as another system;
2. Tampering - the subject violates the integrity of the system or data;
3. Repudiation - the user can hide that he has taken certain actions in relation to the system;
4. Information disclosure - the confidentiality of data in the system has been violated (data is leaked, intercepted);
5. Denial of Service (D.o.S) - an attacker creates conditions under which legal users of the system cannot access its resources;
6. Elevation of privilege - a user who has only limited access to the system can independently expand the accessibility.

The STRIDE model includes three steps: defining the architecture, breaking it down into components, and identifying threats for each component.

Let us consider the operation of the STRIDE model using the example of the functioning of a fragment of the data transmission subsystem in IoT based on new generation 5G (6G) cellular networks (hereinafter referred to as diagrams) [25]. This choice is based on the fact that every day people, companies and government bodies exchange data arrays, often in unencrypted form, without assuming that an outsider can access this data, because by default they trust the protection of their data to the transmission medium of this data [26], and cellular networks of the 5G (6G) standard are promising networks of the future.

The simplified diagram shown in Fig. 5 consists of User Equipment (UE) which is a smartphone, tablet, etc. (usually called an IoT device), a complex of receiving and transmitting antennas (Radio access network (RAN)) and a distributed software and hardware complex - the 5G core.

A more detailed division of the system into components (according to the algorithm of the STRIDE model) makes it possible to identify the main software modules and network functions (Network Function (NF)) of the basic architecture of the 5G network (Fig. 6) [27]:

- User Plane Function (UPF) module for implementing user plane functions;
- Data Network (DN) for organizing operator services, Internet access, etc.;
- Access and Mobility Management Function (AMF - Access and Mobility Management Function);

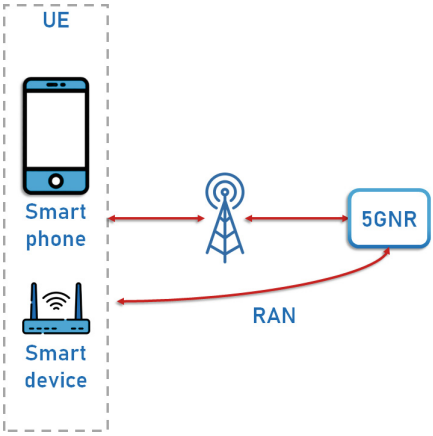

Fig. 5. Simplified diagram of 5G

– Session Management Function (SMF) module;
– Policy control module (Policy Control Function (PCF));
– Unified Data Management (UDM) module;
– Application Function (AF) module.

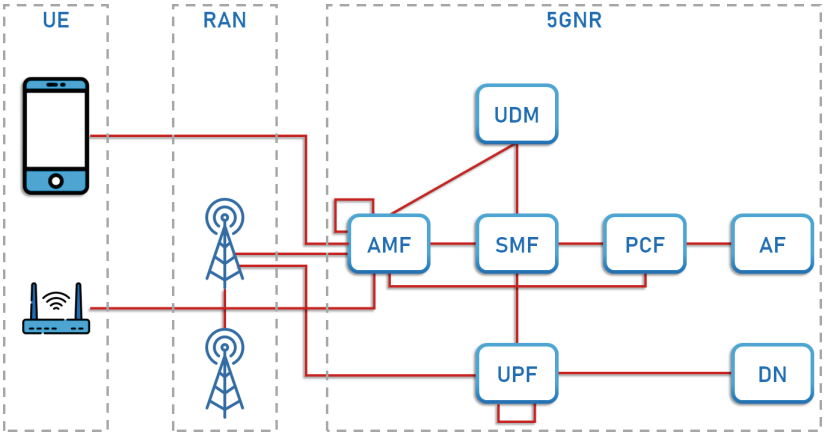

Fig. 6. Detailed diagram of 5G architecture

To make it more effective, the following security management features need to be added [27]:

– Anchor function of safety (Security Anchor Function (SEAF));

- The Authentication Function (AUSF) that acts as an authentication server, terminating requests from SEAF and translating them to the Authentication Credential Repository and Processing Function (ARPF);
- Authentication credential or ARPF repository and processing function;
- Subscription Identifier De-concealing Function (SIDF) function;
- Security Context Management Function (SCMF) function;
- Security Policy Control Function (SPCF) function;

These schemes determine not only information transfer flows between system components, but also provide an opportunity to analyze the process of confidential information circulation in order to understand which components can be attacked. In addition, identifying the boundaries of trust (red dashed line) will help to find possible entry points to potentially vulnerable information flows (Fig. 7).

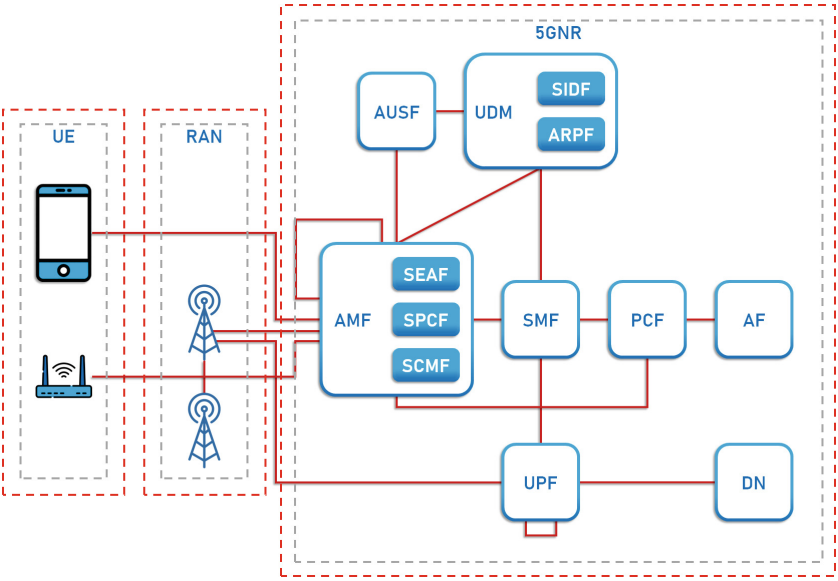

Fig. 7. Detailed 5G Architecture Diagram with Trust Boundaries and Security Modules (Color figure online)

As a result of the detailing and application of the STRIDE model to the components of the 5G network architecture, it is possible to determine a fairly complete list of possible threats to a given fragment of the IoT data transmission network. As for the general requirements for the security of IoT devices, they should be eliminated during development or specified in the documentation.

6 Using ML to Secure the Internet of Things

As noted earlier, machine learning can do things that humans cannot. ML capabilities include providing automation of large-scale analysis, predicting future events, converting raw data into a human-understandable format, developing a real-time recommendation system, device maintenance (IoT), etc. Based on ML, information processing devices that are part of The Internet of Things can detect trends, anomalies, carry out informational and advisory preparation of solutions, and, ultimately, perform the necessary targeted actions for the functioning of IoT devices. A clear example of the effectiveness of ML is the fight against malware that can change shape to avoid detection, and using the traditional signature-based approach makes it very difficult to detect such sophisticated attacks [22].

The analysis based on the results of threat modeling, taking into account the specifics of new generation 5G (6G) cellular networks, allows us to identify the following main areas of application of ML to ensure IoT security:

1. Implementation of machine learning technology into the firewall core of 5G (6G) cellular network infrastructure equipment in order to stop threats in advance, as well as promptly issue recommendations on the application of the necessary security policy for IoT.
2. The use of built-in machine learning models to prevent previously unknown attacks. Signatures become less valuable to prevent them (using ML's self-learning capability).
3. Using ML development to detect anomalies and vulnerabilities, as well as providing full visibility and transparency when connecting new and previously unregistered IoT devices, which is the first step towards building a predictive maintenance system.
4. Implementation of ML technologies in the core of 5G (6G) infrastructure modules in order to reduce the level of errors (including human ones) due to the capabilities of machine learning to analyze huge amounts of telemetry and other data and reduce the response time to threat recognition, etc.

The list of areas of application of machine learning can be significantly expanded if we consider the introduction of ML technology not only to protect the IoT, but also in relation to all levels of ensuring the functioning of the Internet of things, including identification, classification, forecasting, etc. By definition, IoT deals with the interconnection of devices with the primary purpose of exchanging information (data). At the same time, it is this data that is the standard reason that makes machine learning more powerful, increasing the efficiency of IoT [28].

7 Conclusions

The rapidly evolving technologies of the Internet of Things require constant attention to security issues, especially given the serious catastrophic consequences of breaching their protection. To carry out measures to protect IoT,

it is necessary to complete a whole complex, starting with the analysis of possible attacks and building a classification model for possible threats. Considering the trend of further development of IoT devices, it is advisable to focus on ensuring the security of promising information transmission systems based on cellular networks of the 5G (6G) standard, as well as the use of machine learning technology to ensure the security of the Internet of things. In this paper, we have formulated a sequence of steps and a set of technologies that should provide sufficient security for promising IoT systems.

The article was prepared as part of the implementation of the program of strategic academic leadership "Priority-2030", Strategic project No. 2 "Digital transformation of the university and industrial enterprises based on the Intelligent Cyber-Physical Platform".

References

1. "2020 Unit 42 IoT Threat Report," Palo Alto Networks, 10 March 2020. https://unit42.paloaltonetworks.com/iot-threat-report-2020. Accessed 04 Apr 2023
2. Electronic resource. https://www.kaspersky.ru/resource-center/preemptive-safety/best-practices-for-iot-security?ysclid=lg2357k9zr450745102. Accessed 04 Apr 2023
3. Nefedova, M.: Zerobot botnet attacks vulnerable IoT devices Zyxel, D-Link, BIG-IP and more 08.12.2022. https://xakep.ru/2022/12/08/zerobot. Accessed 04 Apr 2023
4. Vereshchagina, E.A., Kapetsky, I.O., Yarmonov, A.S.: 317 Security Issues of the Internet of Things. World of Science, Moscow (2021). Online edition. ISBN: 978-5-6045771-9-6. https://izd-mn.com/PDF/20MNNPU21.pdf. Accessed 27 Mar 2023
5. Global Information Infrastructure, Internet Protocol Aspects and Next Generation Networks: Overview of the Internet of Things, 22 p. ITU (2012). (ITU-T Recommendations; Y. 2060). https://iotas.ru/files/documents/wg/T-REC-Y.2060-201206-PDF-R.pdf. Accessed 27 Mar 2023
6. Tsvetkov, V.: Information interaction. European Researcher. Series A. **62**(11-1), 2573–2577 (2013). http://www.erjournal.ru/journals_n/1386019866.pdf. Accessed 29 June 2023
7. Grammatchikov, A.: In three years, each Russian will have six devices connected to the network. CNews.ru, 21 April 2020. https://www.cnews.ru/articles/2020-04-21_cherez_tri_goda_na_kazhdogo_rossiyanina?ysclid=lfsrgtbgdy268814557. Accessed 29 June 2023
8. Prieto, R., Hunt, E., Cromwell, C.: Cisco Visual Networking Index Predicts Global Annual IP Traffic to Exceed Three Zettabytes by 2021. The Newsroom: Cisco's Technology News Site, 08 June 2017. https://newsroom.cisco.com/press-releasecontent?type=webcontent&articleId=1853168. Accessed 28 Mar 2023
9. Bogdanov, A., Shchegoleva, N., Dik, G., Khvatov, A., Dik, A.: "Smart habitat": features of building it infrastructure, main problems of building data networks using 5G (6G) technologies. In: Gervasi, O., Murgante, B., Misra, S., Rocha, A.M.A.C., Garau, C. (eds.) ICCSA 2022. LNCS, vol. 13380, pp. 628–638. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-10542-5_43
10. Kupriyanovskiy, V.: On standardization of smart cities, Internet of Things and big data. The considerations on the practical use in Russia. Int. J. Open Inf. Technol. **4**(2), 34–40 (2016)

11. Just like ABCDE: how the Internet of Things works. Electronic Resource. https://trends.rbc.ru/trends/industry/5f7ca9f89a79471a3d36cb2c. Accessed 29 Mar 2023
12. Rayes, A., Salam, S.: The things in IoT: sensors and actuators. In: Rayes, A., Salam, S. (eds.) Internet of Things From Hype to Reality, pp. 57–77. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-44860-2_3. Accessed 31 Mar 2023
13. Minerva, R., Biru, A., Rotondi, D.: Towards a definition of the Internet of Things (IoT). IEEE (2015)
14. Veretennikov, A.V.: BigData: big data analysis today, No. 32 (166), pp. 9–12 (2017). https://moluch.ru/archive/166/45354/. Accessed 04 Apr 2023
15. Lee, P.: Architecture of the Internet of Things, 454 p. DMK Press, Moscow (2020). Lee P., trans. from Eng. M. A. Reitman. ISBN: 978-5-97060-784-8
16. Letichevsky, A., et al.: Basic protocols, message sequence charts, and the verification of requirements specifications. Comput. Netw. **49**(5), 661–675 (2005). https://doi.org/10.1016/j.comnet.2005.05.005. Accessed 31 Mar 2023
17. Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures, 103 p. European Union Agency For Network And Information Security, ENISA, Hague (2017). https://doi.org/10.2824/03228
18. Chantsis, F., Stais, I., Calderon, P., Deirmenzoglu, E., Woods, B.: Practical Hacking of the Internet of Things, 480 p. DMK Press, Moscow (2022). Transl. from English. L. N. Akulich
19. Ubozhenko, E., Kruteeva, O., Vdovin, S.: Economic justification for the introduction of digital technology "Internet of Things" in the company's activities. Bull. Altai Acad. Econ. Law **11**(1), 92 (2021)
20. Vlasenko, A.V., Kiselev, P.S., Sklyarova, E.A.: Security of the Internet of Things, No. 21 (363), pp. 86–89 (2021). https://moluch.ru/archive/363/81232/. Accessed 05 Apr 2023
21. Vlasova, Y., Kireev, V.: Review of the Russian market of IoT-technologies. Mod. Sci. Intensive Technol. (8), 48–53 (2018). https://top-technologies.ru/ru/article/view?id=37118. Accessed 05 Apr 2023
22. Glonass, V.: The future of machine learning in cybersecurity. Intersectoral J. Navig. Technol. (2022). http://vestnik-glonass.ru/news/tech/budushchee-mashinnogo-obucheniya-v-kiberbezopasnosti/?ysclid=lgamagzbr866573019. Accessed 10 Apr 2023
23. Riad, R., et al.: Learning strides in convolutional neural networks. arXiv preprint arXiv:2202.01653 (2022)
24. Threats included in the Microsoft Threat Modeling Tool, 27 September 2022. https://learn.microsoft.com/ru-ru/azure/security/develop/threat-modeling-tool-threats. Accessed 10 Apr 2023
25. Tong, W., Zhu, P. (eds.): 6G Networks. The Path From 5G to 6G Through the Eyes of Developers. From Connected People and Things to Connected Intelligence, 624 p. DMK Press, Moscow (2022). per. from English. V. S. Yatsenkova
26. Smelyansky, T. https://cipr.ru/news/kakoe-oborudovanie-neobhodimo-dlya-rossijskih-setej-5g/?ysclid=lgdpc73kar778720058. Accessed 13 Apr 2023
27. What is the 5G network architecture. https://www.shunlongwei.com/ru/what-is-5g-network-architecture/. Accessed 12 Apr 2023
28. Antipko, A.: What tasks can be solved by machine learning, No. 5 (452), pp. 4–6 (2023). https://moluch.ru/archive/452/99591/. Accessed 13 Apr 2023