Cybersecurity and Data Stability Analysis of IoT Devices

Malinovskyi Vadym, Kupershtein Leonid and Lukichov Vitaliy

November 7, 2022

Cybersecurityand Data Stability Analysis ofIoT Devices

Malinovskyi Vadym
Information Protection Department
Vinnitsia National Technical University
Vinnitsia city, Ukraine
vad.malinovsky@gmail.com

Kupershtein Leonid
Information Protection Department
Vinnitsia National Technical University
Vinnitsia city, Ukraine
kupershtein.lm@gmail.com

Lukichov Vitaliy
Information Protection Department
Vinnitsia National Technical University
Vinnitsia city, Ukraine
lukichov.vitalyi@vntu.edu.ua

***Abstract*— the aspects of analysis of modern cyber threats and their stability and reliability problems in Internet of Things devices, as well as stability risks of Internet of Things devices arising in modern personal users devices and Industrial Internet of Things systems, were considered in this paper. The main factors of influencing of the informational intrusions, data stability and also the consequences of their successful manifestation are considered in these papers. The approaches of more stable and secure decision for data environments in IoT were proposed. Development prospects and an approach to reliability assessment of Internet of Things systems and personal usersdevices are considered.**

Keywords*— *The Internet of Things (IoT), stability of operation, communication channels, processing paths, informational influences, cyber threat, cyber security, software.

I. Introduction

Modern devices of the Internet of Things (IoT) [1] are widely cover all spheres of modern peopleslife from household personal use devices to professional industrial systems and devices. The Internet of Things is a number of devices, such as personal mobile userdevices (smartphones, biotrackers, fitness trackers, smartwatches, various devices for portable use) from individual personal use to number of industrial professional devices and nodes, alsoincluding devices, which using Internet connections and interfaces.

IoT devices – are include highly intelligent ICs ,multi level software modules, with high-tech decision and complex system integration components. That provide an additional complex risks factors for their cyber security and stability , that violates it's normal functionality by a complex multilevel risks. IoT microcontrollers and communication and functional ICs in it's schemas as a multilevel difficult architecture with separate links, which also carry additional risks of stability andcybersecurity for mobile operating systems and general IoT functionality.

Modern IoT devices has a significant problem – it'sa complex information security and reliability risks for data in IoT, which affects on the final stability of their data processing and transmitting processes,witch take place inIoT systems. With the growing popularity of smart devices and IoT services, the intensity of cyber threats and reducing of summery reliability is increasing.

The latest modern technologies of Internet of Things devices (IoT, Internet of Things) and BYoD (Bring Your Owned Device) users' personal devices, such as smartphones, fitness bracelets, start watches, personal health monitoring devices, sensors, WiFi and Bluetooth headsets and quite widely cover all spheres of modern life from household personal use to industrial systems of professional specialized direction.

Most modern IoT and BYoD devices are highly intelligent information systems containing multi-bit ARM microcontrollers and accompanying processing and information transmission paths with micro programs and separate mobile operating systems in their composition. This makes it possible to almost completely automate the processes of data processing and exchange through the network and Internet transmission channels, to make work processes comfortable and multifunctional. The latest trends in the implementation of IoT and BYoD technologies of remote monitoring and remote control allow organizing highly efficient, comfortable and automated management, monitoring and data presentation of information systems, for example, the integration of personal devices in the Smart House systems.

The most of modern IoTdevices problem– it's their stability and reliability [2].

The goal of research – is a provide of analysis of main cyber threads and also systematization and development of mathematical model of risk factors in IoT devices.

II. Modern cyber threats and data protection in Internet of Things devices

Modern IoT devices and their architecture are including highly intelligent ICs, multi-levelsoftware including IT high-tech decision and complex software modules. They are containing microcontrollers and communication paths and schemas with separate mobile operating systems or firmware in their composition. Modern IoT has a significant problem – it's complex information security and risks [2] for data and stability of their information processes, witch take place in IoT

979-8-3503-9891-5/22/$31.00

systems. With the growing popularity of smart devices and IoT services, the intensity of cyber threats is increasing. The trends of last years indicate that the main cyber threats in modern IoT are [2]-[11]:

- replacement and modification of the original software modules or it’s components;
- interception, modification and distraction of data in channels and interfaces;
- malicious code and malware modules "injection" and/or intercepted data streams into IoT;
- core of operating systems cyber threats of the IoT platform and in firmware of control schemas with microcontrollers;
- information threats for EDGE-level edge devices (switches, routers, modems, gateways and communication interfaces);
- direct and indirect active and passive cyber attacks and interference in IoT information processes;
- interception of control and/or interception or distortion of data. Exceeding access rights in software modules;
- malware (malicious and modified) IoT software;
- malicious links and phishing resources. IoT attacks;
- web malicious scripts and malicious code in relevant computing environment in IoT.

Therefore, the trends of recent years and the trends of cyber threats indicate that in 2020-2022, a large part of threats (35-44%)has main vector and sourcefrom the global Internet network and their connections, precisely on the Industry Internet of Things (IIoT). 25-44% threats of which is aimed specifically at mobile personal devices (BYoD:Bring You owned Device) and systems with communication capabilities and arranged network interfaces or Internet connection functions. In the times of information confrontation, complex hybrid war and in the future with the development of software tools for carrying out cyber attacks and cyber threats functions, an increase in the number of attacks on industrial and personal IoT devices and on the sphere of Internet devices in general is predicted, covering systems from portable devices of users and "smart home" systems, critical systems and biomedical IoT. The largest IoT vulnerability is violation of security functions of the core level (core) and network (network) interfaces.

Improving of the cybersecurity of mobile platforms and devices is a complex process for difficult IoT infrastructure. The methods and tools of analyses and neutralization cyber threats and modern attacks are also constantly evolving, such as evolved a malicious software and their methods. According to statistics, 4 out of 10 attacks and cyber threats are aimed at personal and IoT devices. The main elements and targets for attacks in IoT systems are:

- LTE/EDGE, GPS, Wi-Fi and Bluetoothinterfaces andtransmission channels with communications drivers and APIs [2];
- Core and input-output software and hardware components on adjacent mobile operating systems of IoT control/monitoring devices;
- replacement of software components and software updates or supplies;
- violation of the mechanism of distinguishing access rights of IoT components;
- imperfections and vulnerabilities (CVE)of mobile devices and their OS;
- lack and vulnerabilities of data protection IPS/IDS software components and components of network protection, such as firewalls of VPN/Proxy channels with the low level of encryption (IP Sec+ RSA) and protection;
- the use of social engineering and phishing methods (such as malicious WEB- links and multimedia files with embed malware or malicious exploits) in IoT software with the subsequent implementation and execution of its exploits and injections of malicious "breakthrough" code to disrupt the standard functionality - the OP core of IoT devices. At the same time, in this case can be used an autostarter zero-click various mechanisms of startsof its exploits, also from the user himself when opening or linking to this resource;
- violation of the ECC memory protection mechanism at the core level of IoT devices (execution of methods of unauthorized access to protected memory areas: buffer overflow, buffer read-write overflow, access to protected memory areas, direct memory access and others);
- violation of the security of border devices and communication interfaces in the device (routers, switches, radio communication equipment, etc.);
- violation of the secure connection mechanism and MITM attack;
- imperfection and cyber threats of the supporting architecture and related devices;
- modern anti-virus software (viruses, trojan horses and backdoors, malicious applications and programs);
- imperfection of network and cloud services, API software interfaces and imperfection of mobile device security settings;
- - uses and exploitation of "0" zero-day information threats and vulnerabilities.

Given such a large number of potentially possible cyber threats and information risks for IoT and mobile personal devices, it is necessary to use comprehensive IoT approaches and mechanisms at all levels. It is also relevant to develop new progressive approaches and world-leading practices, such as demarcation of the network, IoT segments, zero trust area (ZeroTrust), Complex Data Protection System for IoT. The use of a comprehensive method of checking and neutralizing cyber threats is also relevant. In general, the structural mechanism and complex approach to data protection in IoT and its component should include the parallel use of information protection mechanisms:

$$\begin{aligned}&F_{Max}(IoT\ Data\,\mathrm{sec}urity\ KPI) \rightarrow F_{EndPo\mathrm{int}\,IDS/IPS}(t_i, x_i, \in n) + \\ &+F_{EndPo\mathrm{int}\,Component\ Firewall}(t_i, y_i, \in m) + F_{VPN/VPS\,(withIP\,\mathrm{sec})}(t_i, z_i, \in k) + \\ &+F_{RSA\,Sessions}(t_i(t_i \rightarrow t_{i\,\mathrm{min}}), keys[i]) + \\ &+F_{ZeroTrustZonePolicies}(t_i, x_i, \in n, y_i, \in m, z_i, \in k, t_i \rightarrow t_{i\,\mathrm{min}}), \qquad (1)\end{aligned}$$

where F_{Max} *(IoTDataSecurity)* – designation (marking) of a complex function of maximum IoT information protection with a minimum number of threats vectors in data systems of IoT ; $F_{EndPoint\ IDS/IPS}(x_i \epsilon\ n)$ – complex function of anti-virus protection IPS/IDS (IntruderPreventionSystem / IntruderDetectionSystem) based on modern tools of cyber protection and data analysis methods and data protections polices in IoT; $F_{EndPointComponentFirewall}\ (y_i \epsilon\ m)$– functions of modern network screens with a traffic analyzer, SIEM elements and analysis of data flows in IoT network paths; $F_{VPN/VPS(withIPSec\ )}\ (t_i, z_i \epsilon k)$ – functions of using components of a network tunnel with encryption and a secure IPSec transmission protocol; $F_{RSASessions.}\ (t_i,, t_i \rightarrow t_{imin})$ – functions of using cryptographic protection mechanisms and algorithms when exchanging data with encryption keys; $F_{ZeroTrustZonePolicies}$ $(t_i,, x_i \epsilon\ n;\ y_i \epsilon m;\ z_i \epsilon k\ ;\ t_i \rightarrow t_{imin})$ – the use of access rights demarcation policies and information security policies based on the concept of zero trust in IoT zones,t_i,- conditional time intervals; $x_i\ \epsilon\ n\ ;\ y_i \epsilon m\ ;\ z_i\ \epsilon\ k$ –corresponding information parameters and their belonging to sets;$t_i \rightarrow t_{imin}$ –minimal time interval as a criteria for performing functions in the shortest possible time.

In general, it is possible to achieve the maximum level of protection in IoT only with the use of an integrated approach, the use of individual components mentioned above in the above integrated approach and the function of date protection in IoT, under the conditions:

$$F_{Max}(IoT\ Data\sec urity\ KPI) \rightarrow F_{Optimal}(IoT\ Data\sec urity\ KPI) \quad (2)$$

It is very difficult to provide and cover full range of functional security and secure data transmission &processing for personal IoTand mobile personal devices of users as part of it, taking into account the different functional orientation and the use of individual multi-structured components in the complex and multi-component information system of modern IoT, as well as taking into account the specifics of the use of publicly available Internet channels – as one of the main sources of cyber threats.

III. Analysis of the Reliability of Functioning of Modern Devices in the Internet of Things

Second after cybersecurity problem in modern IoT – its their stability and reliability.

The probability of failure-free operation in IoT or BYoD during time t is determined by some reliability function $p(t)$ .The probability that the IoT or BYoD object will fail during time t characterizes the opposite property – unreliability and is expressed as: $q(t) = 1 - p(t)$ .Obviously, $q(t)$ can be considered as a failure distribution function, its derivative: $f(t) = -{}^{dp(t)}\!/_{dt}$. It's the density of the distribution of uptime or, as they say, the density of failures.

The very function of reliability in IoT or BYoD is described by the main elements on which it depends:

$$p(t) = a_0 + \sum_{i=1}^{n}(P_i(t)) = a_0 + \sum_{i=0}^{n} pi(\Delta t). \qquad (3)$$

where $P_i(t)$pi – single component of reliability for each of the factors affecting reliability (described in the list above); $pi(\Delta t)$– unit reliability component for each of the factors at the time interval $\Delta t = t_i - t_{i-1}$.

The model of the IoT or BYoD system, in which the failure of each element occurs independently and leads to the failure of the entire system (simple system), in the sense of reliability. According to the rule of multiplication of probabilities for independent events, the probability of fault-free operation of the system $p(t)$ is equal to the product of probabilities p_i trouble-free operation of its elements $(i = 1, 2, ..., n)$:

$$p(t) = \prod_{i=1}^{n} p_i = \prod_{i=1}^{n} e^{-\Lambda_i(t)} = \exp\left(-\sum_{i=1}^{n}\Lambda_i(t)\right) = \exp\left(-\sum_{i=1}^{n}\int_0^t \lambda_i(t)dt\right). \quad (4)$$

It follows from this that the failure intensity of a simple IoT or BYoD system is equal to sum of its elements failure intensities and connections: $\lambda(t) = \sum_{i=1}^{n}\lambda_i(t)$.

The reliability of modern IoT or BYoD devices is relatively high, covering systems from user portable devices and "smart home" and "smart doctor's office" systems to systems for industrial start-up control of production processes at enterprises, including individual components of automation and telemonitoring and telecontrol in them unreliable elements in the composition of these systems appear mainly due to external reasons and to a greater extent due to security problems or physical impact on these systems. Correspondingly, by improving information protection, you can improve the reliability of IoT or BYoD work, because the degree of protection and consequences directly depends on the stability of the entire systems. The biggest vulnerability for IoT or BYoD is a violation of the security of the core level (Core) at the level of server software modules and its incorrect configurations. Also, the trends of 2020-2022 are attacks on communications and communication channels and communication interfaces of devices using methods of violation of procedures protected data exchange them, as well as software modification and malware injection.

Determination of the intensity of appearance of cyber threats of elements or nodes of the software, taking into account the conditions of operation and the potential environment of use:

$$G(\lambda_i) = \lambda_{0i} \cdot n \cdot K_1 \cdot K_2 \cdot K_3 \cdot K_4 .... \cdot K_{m-1} \cdot K_m = \lambda_{0i} \cdot n \cdot \prod_{i=1}^{m} K_i = \lambda_{0i} \cdot n \cdot K_S. \quad (5)$$

where λ_i , λ_{0i} – nominal actual and initial failure intensity of elements in the event of a cyber threat; K_1,$K_{2,}K_i$ – correction coefficients for the occurrence of cyber thr ats depending on the type of software, the structure and relationships of it's elements, algorithms and the structure of data processing, depending of the influence of influence factors or cyber threats (Ki = 0..1); K_3 – correction factor depending of the conditionsand operation environment of the software system; K_4– correction factor depending on the influence of the intensity of potentially dangerous software(K_3 = 1..1.2, K_4 = 1,45..1.47); n – the number of software elements in the IoT information system.

IV. Reliability of IoT Software Components

The description of the intensity of the emergence of cyber threats in the Internet of Things is determined by the probability of stable operation of software without failures and without threats in a given time interval Δ t_p (0, t_p):

$$P(t) = \exp(-\Delta t \sum_{i=1}^{n} (\lambda_i \cdot k_i)) \quad , \qquad (6)$$

where n –number of block/module elements in the software; λ_i– the intensity of the cyber threat; k_i–the cyber threat occurrence rate for each block.

At the same time, the total intensity of failures due to a cyber threat of a particular software product:

$$\Lambda = \sum_{i=1}^{n} \lambda_i \times 10^{-6} [1/hour] , \qquad (7)$$

We calculate the average time of stable work (work without cyber threat or data intrusions) under the conditions of maintaining full functionality:

$$\mathrm{T_{cs}} = 1/\Lambda, \quad T_{cs} = \frac{1}{\Lambda} \quad \text{[hour]} \qquad (8)$$

We determine the coefficient of preparedness for a cyber threat/cyber attack as Hλi = μ/(μ+λi), where μ – intensity of restoration of software components/modules of loss of functionality in the event of a cyber threat:

$$\mu_s = \sum_{i=1}^{m} \mu_i . \qquad (9)$$

Thus, the stability indicators of the software products in IoT or software system, which consists of modular m – components, obtained as a result of the calculations – the probability of error – free stable operation and the average time of stable operation meet the necessary requirements.

V. Approaches to Ensuring the Security of Information Transmission and Processing Processes in Microcontrollers

Since informational threats in IoT devices architecture, are quite often complex and have a complex nature and stages of implementation, then solutions aimed at protecting the computing andprocessing algorithms must also have a comprehensive approach.

To ensure the closure of potentially dangerous critical places of the IoT architecture, individual and complex approaches are used to organize the necessary state of security [2], [4]-[9]:

- hardware-based approaches that use a cyclic redundancy check calculate, i.e. a checksum is calculated that detects errors in data transmission or storage. Not only does this ensure code integrity is checked, but it also means that the signature can be calculated at runtime;
- monitoring of data parameters and resource is another method with a high degree of protection. To determine the cause of the reset and thereby ensure reset only through authenticated access to the specials flag status management system. Statuses of system health provided by the indicates of specials flags in data security algorithms of system health. All flags are programmable by system monitoring and security tools and their algorithms. For effective manipulation detection and logging, this is complemented by the "Read-Write" function - reading while writing, that is, reading one word while writing another word);
- approaches involving the use of isolation and control of the main core components MCC (Main Core component)provided hardly or by security system functionality;
- control of the integrity and reliability of the memory content, which is provided by checking and correcting errors of the Error Correction Code and checking parity. It also provides additional protection against attacks aimed at preventing code bugs from infecting systems;
- control of external physical and electrical parameters of processors and hardware tracts in IoT. For example, a temperature sensor continuously measures the temperature of the environment surrounding the microcontroller. This is necessary in order to ensure that it remains within the specified range and thus avoid the risk of damage during special prolonged heating;
- development of a cyber defense strategy and new safety methods [12], [13]. The task of developing and implementing an effective cyber defense strategy should include the minimization of each probability and the reduction of each probability for each of the factors, which will lead to a decrease in the overall probability P(λ_i) and an increase in the security of the information system R;
- use of cryptographic systems and data processing algorithms in microcontroller systems with reliable cryptographic protection. This approach requires, in particular, a specialized architecture with cryptographic peripherals (encoder/decoder) and belongs to the number of specialized reliable microcontrollers systems in IoT;
- use of multi-level hardware and software isolation, which includes: isolation of software code and access methods to data streams and streams of software code commands and data; physical isolation of the electrical part of the microprocessor system; information isolation of the microprocessor system; electrical insulation, including electromagnetic isolation of the microcontroller system; secondary noise filtering to/from the MC, electrical isolation and filtering of power lines and data transmission lines from/to external circuits, such as sensors and/or control circuits; verification and careful correlation of the software code before programming/updating for the detection of vulnerabilities in the microcontroller system; checking and monitoring the state of the MK system; the use of data encryption and coding for MK with an increased level of protection (used in protected and cyber-resistant microcontroller systems).
- use of modern innovative approaches of the protection mechanisms of microprocessor and memory systems in IoT: the use of virtualization algorithms of the main computing process. One of such approach and method is proposed multi-level backup by copying/fixing and restoring previous t_{i-1}, t_{i-2} ...t_{i-n} states of the computing process. In the event of a cyber threat, the vector of parameters and the state of the computing process is restored from the previous values of the computing parameters before the cyberattack on IoT system. In the event of a cyber threat, the vector of parameters and the state of the computing process is restored from the previous values in time intervalst_{i-1}; t_{i-2}; t_{i-m}. t_m,etc:

$$f'(t_i, R', x', y', z', t', n', d') \xrightarrow{flc=true} f(t_{i-1}, R, x, y, z, t, n, d);$$
$$R' f(t_i, n'_x \in V') \xrightarrow{flc=true} Rf(t_{i-1}, n_x \in V);$$
$$n_x = \sum_{i=x}^{N} (n_i), \qquad (10)$$

where $f'(t_i, R', x', y', z', t', n', d')$ – the current function of vector data parameters of the computing process in threated IoT system in actual time t_i (after intruded of cyber threat); $f(t_{i-1}, R, x, y, z, t, n, d)$ –the current function of vector data parameters of normal state computing process in normal IoT system in previous time t_{i-1} (before intruded of cyber threat); $R' f(t_i, n'_x \in V')$ – information model of threated IoT system; $Rf(t_{i-1}, n_x \in V)$ –information model of normal IoT system; $n'_x \in V' \, n_x \in V$ –the number and plural of n_x – data parameters of information model of IoT system; $t_{i-1} t_i$ – previous and current (actual) time; flc –flag of cyber threat. x, y, z, t, n, d – the value of data parameters of the function of the computing process in IoT .

This approach as part of the method is implemented by restoring the previous state of the computational process in IoT data system, which can be described by the right-hand part of the upper expression of formula (10).This investigation by restoring the parameters and it'svalues of the function from saved copies and parameters of the function of previous values in memory and using other additional methods and means.

The disadvantage of this approach is the need for a significant amount of additional resources of the microcontroller, including memory to reserve previous states of the computing process.

To protect against information interference and intrusions by cyberattacks and cyber threats in IoT microcontrollers and architecture this approaches must be implements in automated and automatic mode, as well as other software technologies in IoT devices in the context of modern approaches of Industry X.0.Cyber-physical systems, complex protection approaches are becoming more and more relevant, including protection of the hardware perimeter of the IoT devices connection and interference in the operation of microprograms and software. The main efforts are directed to the protection of firmware, memory and microcontrollers in IoT. But not enough effort and attention is paid to the protection of information interference through secondary channels and lines of communication in this devices. Modern approaches provide for the definition and use of protected zones and the perimeter of IoT devices connections. Solutions are used in the field of authentication and cryptographic protection of the IoT environment, the use of "0"(zero) trust zones during the operation of the IoT platform and interaction with other modules – as a most reliable way to provide IoT cybersecurity.

VI. Summary and Conclusion

Providing of the stability and reliability of functionality, the concept of data integrity, availability and confidentiality in modern IoTs and BYoDs is one of the priority tasks. New models and methods should be based on a complex combination of functionality with data virtualization technologies, the use of modern IDS/IPS with mixed additional functionality, methods of separate access levels and resources levels. Also, in order to increase the level of security, additional conditions for checking and controlling third-party information flows with reliable improved encryption with offset and in combination with computing parallelism should be created process with delineation of access rights at different levels of computing and virtual computing environments (shells) for different processes.

Today, in the century of the digital age of information technologies, in the conditions of information confrontations and modern information challenges, for every user of a personal device and users of IoT as a whole, solving the problem of data security in IoT is a basic and main task.

Solving of this two problems (cybersecurity and stability) is possible by using complex approaches to information reliability and security at different levels. This will allow the further development of the IoT and BYoD industry with their safe, stable functioning and introduction into other, ever-widening spheres of life, including use in critical farm systems.

The results are has a systematization mathematical model of risk factors in IoT devices, which can determine of stability parameters of IoT devices by evaluation of reliability indexes (parameters). The given approaches and model can provide a more safety and security modes of operations of IoT devices.

References

[1] V. S .Kharchenko et al,"Internet of Things for Industry and Human Application. Fundamentals and Technologies". *Ministryof Education and Science of Ukraine, National Aerospace University KhAI*, vol. 1, 2019.

[2] V.V.Sklyar, V.V.Yatskiv, N.G.Yatskiv,"Dependability and SecurityInternet of Things: Practicum", *Ministry of Education and Science of Ukraine, National Aerospace UniversityKhAI,Ternopil National Economic University*, 2019.

[3] Speculative Processor Vulnerability. ARM Developer Forum, [online]Available:https://developer.arm.com/Arm%20Security%20Center/Speculative%20Processor%20Vulnerability.

[4] Cache Speculation Side-channels white paper.ARM Developer Forum,[online]Available:https://developer.arm.com/documentation/102816/0205/.

[5] Kernel Side-Channel Attack using Speculative Store Bypass - CVE-2018-3639, [online] Available: https://access.redhat.com/security/vulnerabilities/ssbd.

[6] S.Yegulalp,"Rowhammer hardware bug threatens to smash notebook security",*InfoWorld*, 2015, [online]Available:https://www.infoworld.com/article/2894497/row hammer-hardware-bug-threatens-to-smash-notebook-security.html.

[7] C. Canella, J. Van Bulck, M. Schwarz, M. Lipp, B. von Berg, P. Ortner, F. Piessens, D. Evtyushkin, and D. Gruss, "A systematic evaluation of transient execution attacks and defenses," *arXiv preprint arXiv:1811.05441*, 2018, [online]Available:https://doi.org/10.48550/arXiv.1811.05441.

[8] G. Chen, S. Chen, Y. Xiao, Y. Zhang, Z. Lin, and T. H. Lai, "SgxPectre Attacks: Stealing Intel Secrets from SGX Enclaves via Speculative Execution", *arXivpreprint arXiv:1802.09085*, 2018, [online]Available:https://doi.org/10.48550/arXiv.1802.09085.

[9] V. Kirianskyand C. Waldspurger, "Speculative Buffer Overflows: Attacks and Defenses", *arXivpreprint arXiv:1807.03757*, 2018, [online]Available:https://doi.org/10.48550/arXiv.1807.03757.

[10] C. Chio, D. Freeman,"Machine Learning and Security. Protecting Systems with Data and Algorithms",*O'relly Media Inc.*, 2018.

[11] O. Voitovych, Y. Baryshev, E. Kolibabchuk and L. Kupershtein, "Investigation of simple Denial-of-Service attacks", *2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T)*, 2016, pp. 145-148, [online]Available:https://doi.org/10.1109/INFOCOM-MST.2016.7905362.

[12] O. Voitovych, L. Kupershtein, O. Shulyatitska and V. Malyushytskyy, "The authentication method in wireless sensor network based on trust model",*2017 IEEE First Ukraine Conference on Electrical and Computer Engineering (UKRCON)*, 2017, pp. 993-997, [online]Available:https://doi.org/10.1109/UKRCON.2017.810039.

[13] O. Voitovych, L. Kupershtein, V. Lukichov and I. Mikityuk, "Multilayer Access for Database Protection"*2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, 2018, pp. 474-478, [online]Available:https://doi.org/10.1109/INFOCOMMST.2018.86 32152.