Model of Information Technology for Efficient Data Processing in Cloud-based Malware Detection Systems of Critical Information Infrastructure

Sergiy Gnatyuk[1,2,3], Feruza Satybaldiyeva[4], Viktoriia Sydorenko[1], Oksana Zhyharevych[5], and Artem Polozhentsev[1]

[1]National Aviation University, 1 Liubomyra Huzara ave. Kyiv, 03058, Ukraine
[2]State Scientific and Research Institute of Cybersecurity Technologies and Information Protection Kyiv, Ukraine
[3]Yessenov University, 32 Microdistrict, Aktau, 130000, Kazakhstan
[4]Satbayev University, 22 Satpaev str., Almaty, 050000, Kazakhstan
[5]Lesya Ukrainka Volyn National University, 13 Voli ave. Lutsk, 43025, Ukraine

Abstract

The rapid development of ICT caused significant changes in the ways and means of communication between people using network technologies. Creating, storing, distributing, and sharing information is becoming increasingly easy and accessible. Today, one of the most promising technologies for storing information and providing effective online services is the use of cloud systems. Using this technology to protect computer systems from cyberattacks can bring many advantages compared to traditional protection schemes. However, the rapid evolution of malicious software and the diversification of its types leads to a significant increase in the vulnerabilities of the implementation of attacks on information resources, especially on objects of the state's critical infrastructure. Thus, there is a need to develop new methods and models for effective data processing in cloud-based malware detection systems. In this study, the information technology model for efficient data processing in cloud-based malware detection systems was developed, which considers the need to formulate commands for transferring control to the ICT software client. In addition, a study of the probabilistic and temporal characteristics of algorithms and programs for generating and processing metadata in a cloud-based malware detection system was conducted. This allowed for increasing the accuracy of the results of estimation of time characteristics by up to 1.7 times and jitter characteristics by up to 4.5 times.

Keywords

Malware, malware detection, critical infrastructure, critical information infrastructure, cloud computing, information technology, model for efficient data processing, ICT.

1. Introduction

Up-to-date malware detection technologies include sophisticated mathematical methods as well as hardware and software complexes for data storage, processing, transmission, computerized control, telecommunications, etc. The constant development of computing facilities and automation complexes, as well as the increasing demand for cloud-based malware (Figs. 1 and 2) detection systems, leads to an increase in the volume of metadata transferred to these systems. However, increasing requirements for the accuracy of modeling and quality of technical developments require consideration of many objective and subjective factors (especially important for government critical infrastructure) that arise in the process of ICT operation. The increasing requirements for the accuracy of modeling and the quality of technical developments, however, require the consideration of many objective and subjective factors (especially important for government critical

CPITS 2023: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2023, Kyiv, Ukraine
EMAIL: s.gnatyuk@nau.edu.ua (S. Gnatyuk); feruza201200@gmail.com (F. Satybaldiyeva); v.sydorenko@ukr.net (V. Sydorenko); zhyharevych.oksana@vnu.edu.ua (O. Zhyharevych); artem.polozhencev@gmail.com (A. Polozhentsev)
ORCID: 0000-0003-4992-0564 (S. Gnatyuk); 0000-0003-4107-7568 (F. Satybaldiyeva); 0000-0002-5910-0837 (V. Sydorenko); 0000-0002-1979-4168 (O. Zhyharevych); 0000-0003-0139-0752 (A. Polozhentsev)

infrastructure) that arise in the process of ICT operation:

- The heterogeneity of ICT, which contain diverse components, many of which are themselves complex, multifunctional systems.
- The multi-connected and large-scale nature of ICT.
- The distributed nature of information and computing resources across the global network.
- Susceptibility to various types of external and internal intrusions (especially virus attacks).
- Knowledge-intensive and continuous evolution based on advanced technology and software developments etc.

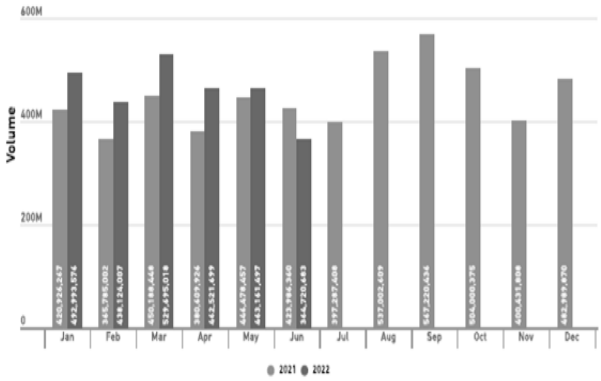

Figure 1: Malware volume in the world in 2021 and the first part of 2022 [1]

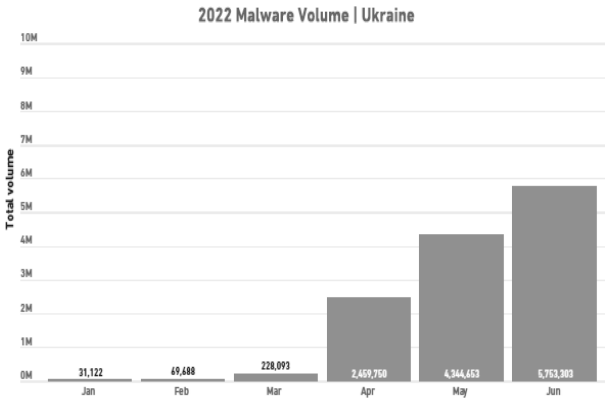

Figure 2: Malware volume in Ukraine in the first part of 2022 [1]

Therefore, there is a problem of developing mathematical models that most accurately formalize the technology of ICT functioning. Especially important is the task of mathematical description of the cloud system technology to detect malware in the ICT, considering some basic factors (heterogeneity, multi-connectivity, etc.).

2. Analysis of Modern Approaches and Problem Statement

Today, cloud computing is one of the most advanced technologies for storing information and providing efficient online services. Using this technology to protect computer systems from cyber-attacks can offer many advantages over traditional protection schemes, such as simplicity, accessibility, lower cost, and scalability. Malware is defined as any malicious software that targets a computer system to perform cyber-attacks to damage endpoints. According to [2], protected assets can include all desktop and laptop computers, computer systems and networks, mobile devices, the Internet of Things (IoT), Cyber-Physical Systems, and the most critical assets of the nation's critical information infrastructure (Fig. 3).

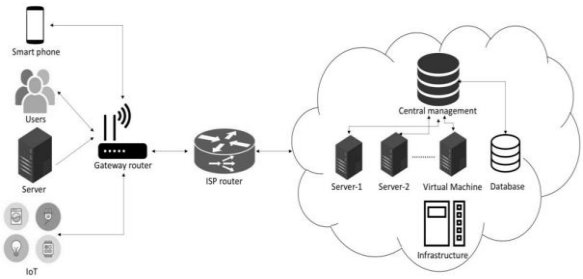

Figure 3: The infrastructure of a typical cloud environment

Let's take a closer look at some studies on malware detection in the cloud environment.

In [3], an approach to protect IoT devices from local computer network attacks is presented. The authors propose a new concept of Behavior-based Deep Learning (BDLF) embedded in the cloud platform of the IoT environment. In this approach, behavior graphs are first built by analyzing API calls. Then, high-level features of the behavior graphs are extracted using stacked autoencoders neural networks. Experimental results show that the proposed BDLF can learn a variety of malware semantics and further improve the average detection accuracy by 1.5%.

In [4], a malware detection method is presented which analyzes the network traffic and software behavior. This method is based on the classification of the sets of API calls used, the frequencies and sequences of API calls extracted from the control flow graphs of software applications, and the features extracted from the

DNS traffic of the network. The results of the experiment showed the reliability of malware detection at the level of 97.29 to 99.42%, which proves the ability of the method to increase the reliability of malware detection.

In [5], the authors proposed an energy-efficient hosting model consisting of individual components of Amazon cloud services to improve the uniqueness and scalability of the model. This study considered the establishment of key benchmarking metrics and known antiviruses for the cloud hosting model. According to the paper, the proposed approach was not only successful for the hosted detection system but also outperformed traditional antiviruses. However, the malware detection infrastructure and hosting model can be further improved by integrating an intrusion detection engine supported by the cloud environment.

In [6], a cloud-based malware detection and neutralization system for wireless multimedia systems in IoT is proposed based on a dynamic differential game. According to the proposed model, firstly, an SVM-based malware detection model is created by sharing data on the security platform in the cloud. Then, the number of malware-infected devices that can physically infect critical nodes is calculated according to the attributes of the Wireless Multimedia System (WMS). Finally, the state transition between WMS devices is described by a modified epidemic model, and a Hamiltonian function has been introduced to simplify the saddle-point solution. In addition, the objective value function and the dynamic differential game were sequentially derived for the Nash equilibrium between the WMS system and the malware. According to the paper, the results showed that the proposed algorithm can neutralize malware accurately and efficiently and is suitable for WMS with limited resources.

In the study [7], the authors proposed an information technology for malware detection in the cloud environment based on Machine Learning (ML). First, they used random simulation to get the worst-case logarithmic loss and then used some models such as KNN, LR, etc. Next, they looked at the logarithmic loss of each algorithm and determined if it was the perfect model. Finally, they deployed the ML model with a user interface on the AWS cloud. According to the authors, they found a unique solution by working with both machine learning and cloud computing to determine the legitimacy of a file. However, this research can be improved by using different data mining techniques to select features or by implementing new learning models.

In [8], a cloud-based malware detection solution called TrustAV is presented. This solution is based on a pattern-matching method to identify contaminated data. TrustAV outsources the processing of malware analysis to a remote server and is offered as a cloud-based solution. According to the paper, TrustAV can protect the transmission and processing of user data even in untrusted environments. In addition, TrustAV uses various techniques offered by Intel SGX technology to overcome common performance issues and limit risk. However, no real-world data is available to evaluate the proposed TrustAV cloud solution.

To detect the rapidly increasing number of malware attacks, an intelligent system based on behavioral analysis in the cloud environment has been proposed in [2]. It creates a dataset of malware on different virtual machines, which effectively identifies distinctive features (Fig. 4).

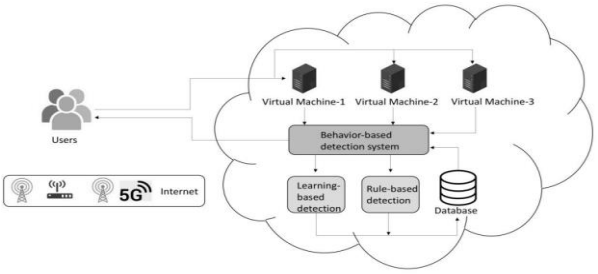

Figure 4: Cloud-based malware detection architecture

Then, samples selected based on training and rules are provided to detection agents to separate such software from safe samples. The authors emphasize that the developed system can effectively detect both known and unknown IPSs with a high level of detection and accuracy. In addition, the results of the proposed method outperform those of the leading methods in the literature. The detection results reach 99.8%, 0.4% false positive rate, and 99.7% accuracy. The proposed system can help those who want to develop a new malware detection system in a cloud environment.

In Table 1, the results of the analysis of malware detection approaches in the cloud environment are

summarized by the following criteria (proposed by authors and based in last advances in the area):

1. Clarity of formalization
2. Flexibility and versatility
3. Ability to self-learn and improve
4. Detection accuracy
5. Experimental validation.

The common goal of all the above studies is to identify malware by increasing the detection rate while reducing the misclassification rate. In reviewing these studies, it is clear that while each detection method has its advantages and works better for certain datasets in a cloud environment, none of them can detect 100 percent of malware.

Table 1
Analysis of malware detection approaches in the cloud environment

№	Approach name	Criteria				
		1	2	3	4	5
1	A deep learning behavioral graph approach to malware detection	+	-	+	+	+
2	Method for malware detection through analysis of network traffic and in-system software behavior	-	-	+	+	+
3	Cloud-based energy-efficient hosting model for malware detection	-	+	+	-	-
4	A dynamic differential game-based malware detection and neutralization model for a wireless IoT system	+	+	+	-	+
5	ML-based malware detection technology for the cloud environment	+	+	+	-	-
6	TrustAV model for detecting malware in the cloud	+	+	+	-	-
7	Malware detection system based on behavioral analysis in the cloud environment	+	-	+	+	+

The purpose of this study is to create and investigate a mathematical model of information technology for efficient data processing in cloud-based malware detection systems in critical information infrastructure.

3. Information Technology Structure of Cloud-based Malware Detection System

Studies of the process of collecting, storing, and processing metadata in cloud-based malware detection systems have shown that the overall structure can be represented as a diagram in Fig. 5.

Let's closely investigate the function of each block.

The data stream from the communication channels arrives at the telecommunications adapter (network application), the main task of which is to separate individual applications from the data stream and form files (control transfer commands) for processing in the software client, as well as the smooth transfer of metadata to the communication channel of the ICT.

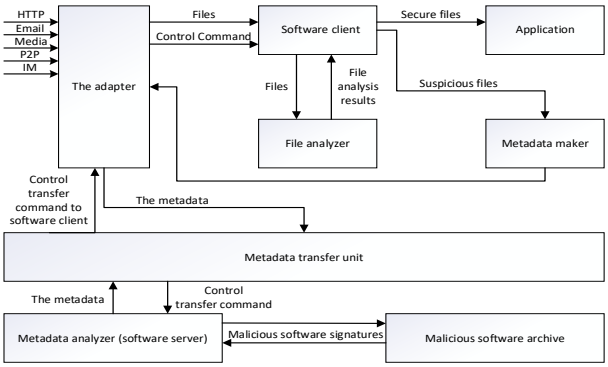

Figure 5: Flowchart of the cloud-based malware detection system technology

The software client is a module that resides on the client's computer and is designed to organize the interaction between the hardware and software components of the system, present suspicious files to the metadata generator, and present the results of the cloud-based malware detection system in a convenient format (creating tables, graphs, charts, etc.). The software client is functionally linked to the file analyzer, which is a software package designed to perform pre-signature and heuristic analysis (comparison with established benchmarks, checking the validity of values, etc.) on the client side of the system.

The metadata generator is designed to extract special signatures from suspicious files using modern file hashing tools. The special signatures are transferred to the communication channel of

the ICT network via the adapter described above. The transmission in the ICT network through intermediate switching nodes (metadata transfer unit) is carried out according to known protocols and advanced methods of information traffic management.

The cloud-based metadata analyzer identifies threats, checks the quality of the decisions made for errors, and then looks for sources of threat propagation. Found sources are also automatically validated to ensure there are no false positives. Information about newly discovered threats and their sources is immediately added to the malware archive and made available to all other users of the product.

Malware data is used to train the metadata analyzer, allowing it to quickly respond to the latest malware developments and automatically detect active threats on users' computers. Infection information used for self-learning includes signature-based and heuristic detection results.

The cloud protection system collects and processes suspicious activity data from every member of the network, providing a powerful expert system for analyzing cybercriminal activity. The data needed to block an attack on a user's machine is shared across the cloud network, preventing further infections.

Studies have shown that the implementation of multi-user distributed applications requires the provision of a socket interface.

A socket is one of the ways that computers transfer data and share information. Sockets are the software endpoints of a network connection. To work with sockets, it is necessary to use a protocol based on TCP/IP and *Windows* transport layer program port. There are three main types of sockets [9]. Client-side sockets initialize a client-side connection to a server-side socket on a remote computer. To open the connection, the client socket must "know" the IP address of the remote machine and the port number used by the server socket. The client sends a connection request to the server. Server sockets themselves do not connect to client sockets. This task is performed by listening sockets embedded in the server sockets. A new client connection request is received by the listening socket, which places it in a queue. When the server socket is released from its current job, it processes the request from the queue and creates a listening socket for the new connection. Server sockets connect to a client socket in response to its request. The client socket receives a description of the server socket, after which the connection is considered established [10–11].

Below is a mathematical formalization of the technology of metadata transfer and processing in cloud-based malware detection systems, and the main temporal characteristics of these processes.

4. Assessing Metadata Processing Time in a Cloud-Based Malware Detection Analyzer

The time of metadata processing in the cloud analyzer is defined by finding the sum of a random number of independent random variables $\xi_1, \xi_2, \ldots$ with the same distribution F and the derivative function of moments $M(s)$. Let N be an integer random variable with a derivative function $A(s) = \sum P_i s^i$ and independent of all of the ξ_j. Then, the random sum of $\xi_1 + \ldots + \xi_N$ has the distribution described by the derivative function of moments

$$\chi(s) = W(M(s)), \qquad (1)$$

where $W(s)$ is a derivative function which describes the random number of metadata items requested by the software client, $M(s)$ and is a derivative function of moments which describes the random processing time per metadata item.

Let's consider the method of calculating the processing time when the number of metadata elements requested by the program client is described by a uniform distribution with integer values. The number of parameters in the task can vary from h to l. The derivative function of the moments of this distribution, considering that all events are equiprobable with the value $\bar{p}$, is equal to

$$M(s) = \bar{p}(e^{hs} + e^{(h+1)s} + \ldots + e^{(l-1)s} + e^{ls}) = \\ = \frac{(\bar{p}(e^{hs} - e^{(l+1)s}))}{(1 - e^{s})}.$$

The derivative function of this distribution is

$$W(s) = \frac{(\bar{p}(s^{h} - s^{(l+1)}))}{(1 - s)}.$$

To estimate the random processing time of a metadata item, a uniform continuous distribution with parameters a and b must be used Then, according to c (1) $\chi(s)$ can be calculated as

$$\chi(s)=\overline{p}\left(\frac{\left(\frac{e^{as}-e^{bs}}{(a-b)s}\right)^{h}-\left(\frac{e^{as}-e^{bs}}{(a-b)s}\right)^{l+1}}{1-\frac{e^{as}-e^{bs}}{(a-b)s}}\right). \quad (2)$$

By differentiating $\chi(s)$ concerning s and setting it equal to zero in the resulting expressions, the first and second moments μ_1, μ_2 concerning the origin are obtained, which correspond to the mean t_s and the variance D of the processing time of a single metadata element transmitted at the request of the software client:

$$\mu_1=t_{cp}^{(o)}=\frac{\partial(\chi(s))}{\partial s}\bigg|_{s=0}=\frac{(h+1)(a+b)}{4}, \quad (3)$$

$$J^{(o)}=\mu_2-\mu_1^2=\frac{\partial(\chi(s))}{\partial s^2}\bigg|_{s=0}-\left(\frac{\partial(\chi(s))}{\partial s}\bigg|_{s=0}\right)^2= \\ =\frac{(h+1)(b-a)^2}{24}, \quad (4)$$

in the case when a metadata analyzer performs processing of files of different, independent information flows, the number of software client requirements for formation, analysis, and processing of control commands can be described by the Poisson distribution [12–14].

In such a case, the derivative function of the Poisson distribution will be as follows:

$$W(s)=e^{\lambda s-\lambda}.$$

Hence, the derivative function of the time moments of the formation of control commands and the execution of the task of the client program is equal to the:

$$\chi(s)=e^{\left(-\lambda+\lambda\frac{e^{as}-e^{bs}}{(a-b)s}\right)}. \quad (5)$$

From (5) the average execution time of the control command generation task and its variance can be found:

$$t_{cp}^{(\phi)}=\frac{\lambda(a+b)}{2}, \quad (6)$$

$$J^{(\phi)}=\frac{\lambda(a^2+ab+b^2)}{3}. \quad (7)$$

5. The Model Simulation Results and Discussion

Let's analyze the mutual influence of the time characteristics given in (2), (4), (6), and (7) on the total processing time of metadata and the formation of control commands.

Fig. 6 shows graphs of the total time $t_{cp}(s)$ (Graph 1) and metadata processing time $t_{cp}^{(o)}(s)$ (Graph 2) (Fig. 4 a-b) as well as graphs of jitter $D(s)$ of total time—(Graph 1) and metadata processing time $D^{(o)}(s)$ —(Graph 2) in conditions when $a=0,4;\ b=0,7;\ h=0,3;\ l=1;\ p=0,3;$ $\lambda=1200.$

The graphs show that considering the temporal characteristics of the formation of control signals will increase the accuracy of the results of the evaluation of temporal characteristics to 1.7 times, and the characteristics of jitter to 4.5 times.

Therefore, a mathematical model of ICT was developed and studied, which allows the evaluation of temporal characteristics of the processing of a metadata element and generation of a control command. The peculiarity of the model is that it considers the necessity of forming control transfer commands to the ICT software client, which generally increases the accuracy of the mathematical modeling results in the considered conditions [15–21].

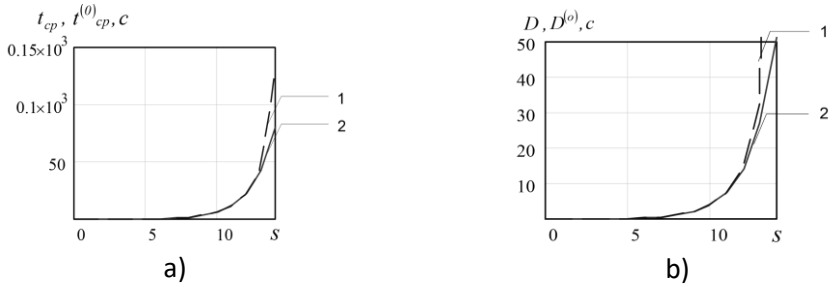

Figure 6: Dependence graphs of $t_{cp}(s)$, $t_{cp}^{(o)}(s)$, $D(s)$ and $D^{(o)}(s)$

In most cases, the probability density distribution of the processing time for a single metadata element and the generation of a control command has a single mode. Formulas (2) and (6) can be used to pre-estimate the spread of the distribution based on the "three sigma" rule. At the same time, the need to take into account the factors mentioned at the beginning of the article requires the development of more complex models, for which the authors will use the GERT structure graph approach in the future.

This will optimize the structure of the metadata creation, transmission, and processing system, as well as the formation of control transfer commands, and evaluate its performance and scalability when increasing the volume and complexity of the tasks to be solved.

It can provide cybersecurity [22–25] from the viewpoint of malware detection and prevention. This is only one side (subdomain) of cybersecurity [26–28].

6. Conclusions

The study analyzes the existing approaches to malware detection in the cloud environment, summarized according to the following criteria: clarity of formalization, flexibility and versatility, ability to self-learn and improve, detection accuracy, and experimental validation.

It is found that all the above studies are to identify malware by increasing the detection rate while reducing the misclassification rate. And while each detection method has its advantages and works better for certain datasets in a cloud environment, none of them can detect 100% of malware.

In this study, the information technology model for efficient data processing in cloud-based malware detection systems was developed, which considers the need to formulate commands for transferring control to the ICT software client.

In addition, a study of the probabilistic and temporal characteristics of algorithms and programs for generating and processing metadata in a cloud-based malware detection system was conducted. This allowed for increasing the accuracy of the results of estimation of time characteristics by up to 1.7 times and jitter characteristics by up to 4.5 times.

7. References

[1] Mid-Year Update: 2022 SonicWall Cyber Threat Report, 39 p.

[2] Ö. Aslan, M. Ozkan-Okay and D. Gupta, Intelligent Behavior-Based Malware Detection System on Cloud Computing Environment, IEEE Access 9 (2021). doi:10.1109/ACCESS.2021.3087316

[3] F. Xiao, et al., Malware Detection Based on Deep Learning of Behavior Graphs, Math. Probls. Eng. (2019). doi:10.1155/2019/8195395

[4] K. Bobrovnikova, D. Denysyuk, Method of Detecting Malicious Software by Analyzing Network Traffic and Software Behavior in Computer Systems, Bull. Khmelnytskyi Natl. Univ. 1(4) (2020) 7–11.

[5] Q.K.A. Mirza, I. Awan, M. Younas, A Cloud-Based Energy Efficient Hosting Model for Malware Detection Framework, IEEE Global Communications Conference (GLOBECOM), 2018, 1–6.

[6] W. Zhou, B. Yu, A Cloud-Assisted Malware Detection and Suppression Framework for Wireless Multimedia System in IoT Based on Dynamic Differential Game, China Commun. 15(2) (2018) 209–223. doi:10.1109/CC.2018.8300282

[7] P. Indirapriyadarsini, et al., Malware Detection Using Machine Learning and Cloud Computing, Int. J. Res. Appl. Sci. Eng. Technol. 8(6) (2020) 101–104. doi:10.22214/ijraset.2020.6015

[8] D. Deyannis, et al., TrustAV: Practical and Privacy Preserving Malware Analysis in the Cloud, 10th ACM Conference on Data and Application Security and Privacy, 2020, 39–48.

[9] S. Mondal, et al., An Improved Methodology for High Frequency Socket Performance Characterization, 2022 IEEE 31st Conference on Electrical Performance of Electronic Packaging and Systems (EPEPS), San Jose, CA, USA, 2022, 1–3, doi:10.1109/EPEPS53828.2022.9947155

[10] M. Rokonuzzaman, et al., Design and Implementation of an IoT-Enabled Smart Plug Socket for Home Energy Management, 2021 5th International Conference on Smart Grid and Smart Cities (ICSGSC), Tokyo, Japan, 2021, 50–54. doi: 10.1109/ICSGSC52434.2021.9490420

[11] R.C. Ooi et al., High Density Interconnect (HDI) Socket Flow & Waprage Prediction & Characterization, 2022 IEEE 24th Electronics Packaging Technology Conference (EPTC), Singapore, Singapore, 2022, 632–638. doi:10.1109/EPTC56328.2022.10013256

[12] Z. Zhang, et al., Research and Analysis about the Length of Vertex-Degree Sequence of Complex Networks with Poisson Distribution, 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), Guangzhou, China, 2017, 28–31. doi:10.1109/CSE-EUC.2017.16

[13] A Poisson Process Model for Monte Carlo, Perturbations, Optimization, and Statistics, MIT Press, (2017) 193–231. doi: 10.7551/mitpress/10761.003.0008

[14] D.K. Sharma, et al., An Efficient Python Approach for Simulation of Poisson Distribution, 2021 7th International Conference on Advanced Computing and Communication Systems, Coimbatore, India, 2021, 2011–2014. doi: 10.1109/ICACCS51430.2021.9441895

[15] O. Solomentsev, et al., Data Processing in Case of Radio Equipment Reliability Parameters Monitoring, 2018 Advances in Wireless and Optical Communications (RTUWO), 2018, 219–222. doi:10.1109/RTUWO.2018.8587882

[16] O.C. Okoro, et al., Optimization of Maintenance Task Interval of Aircraft Systems, Int. J. Comput. Netw. Inf. Secur. 14(2) (2022) 77–89. doi: 10.5815/ijcnis.2022.02.07

[17] J. Al-Azzeh, et al., A Method of Accuracy Increment Using Segmented Regression, Algorithms, 15(10) 378 (2022) 1–24. doi:10.3390/a15100378

[18] F. Kipchuk, et al., Assessing Approaches of IT Infrastructure Audit. In 2021 IEEE 8th International Conf. on Problems of Infocom-munications, Science and Technology (PICST), 2021. doi:10.1109/picst54195.2021.9772181

[19] V. Grechaninov, et al., Decentralized Access Demarcation System Construction in Situational Center Network, Workshop on Cybersecur. Provid. Inf. Telecommun. Syst. II, 3188(2), (2022) 197–206.

[20] O. Solomentsev, et al., Sequential Procedure of Changepoint Analysis During Operational Data Processing, 2020 IEEE Microwave Theory and Techniques in Wireless Communications, 2020, 168–171, doi:10.1109/MTTW51045.2020.9245068

[21] O. Solomentsev, et al., Data Processing Method for Deterioration Detection During Radio Equipment Operation, 2019 IEEE Microwave Theory and Techniques in Wireless Communications (MTTW), 2019, 1–4, doi:10.1109/MTTW.2019.8897232

[22] V. Grechaninov, et al., Formation of Dependability and Cyber Protection Model in Information Systems of Situational Center, Workshop on Emerging Technology Trends on the Smart Industry and the Internet of Things, 3149 (2022) 107–117.

[23] S. Gnatyuk, et al., New Secure Block Cipher for Critical Applications: Design, Implementation, Speed and Security Analysis, Advances in Intelligent Systems and Computing, 1126 (2020) 93–104.

[24] M. TajDini, V. Sokolov, P. Skladannyi, Performing Sniffing and Spoofing Attack Against ADS-B and Mode S using Software Define Radio, International Conf. on Information and Telecommunication Technologies and Radio Electronics, 2021. doi:10.1109/ukrmico52950.2021.9716665

[25] V. Sokolov, P. Skladannyi, H. Hulak, Stability Verification of Self-Organized Wireless Networks with Block Encryption, Workshop on Cybersecurity Providing in Information and Telecommunication Systems, 3137 (2022) 227–237.

[26] S. Gnatyuk, Critical Aviation Information Systems Cybersecurity, Meeting Security Challenges Through Data Analytics and Decision Support, NATO Science for Peace and Security Series, D: Information and Communication Security. IOS Press Ebooks, 47(3) (2016) 308–316.

[27] R. Odarchenko, et al., Improved Method of Routing in UAV Network, Proceedings of the 2015 IEEE 3rd International Conference on Actual Problems of Unmanned Aerial Vehicles Developments (APUAVD), Kyiv, Ukraine, October 13–15, 1, 2015, 294–297.

[28] B. Alsulami, et al., Lightweight behavioral malware detection for windows platforms, 12th International Conference on Malicious and Unwanted Software, Fajardo, PR, USA, 2017, 75–81. doi:10.1109/MALWARE.2017.8323959.