Machine Learning Based Techniques for Cyberattacks Detection in the Internet of Things Infrastructure

Kira Bobrovnikova[a], Sergii Lysenko[a], Ivan Hurman[a], and Andrzej Kwiecień[b]

[a] *Khmelnytskyi National University, Institutska str., 11, Khmelnytskyi, 29016, Ukraine*
[b] *Silesian University of Technology, Poland*

Abstract

The emergence of the concept of the Internet of Things has revolutionized many economic sectors and areas of human activity. At the same time, the spread of the Internet of Things has led to the emergence of cyber security risks in those areas of human activity for which cyber security problems were not relevant before. Most of the security problems in IoT infrastructure arise from a lack of basic security controls. In particular, open ports, security issues with the protocols used in the IoT infrastructure, outdated applications and components of IoT devices, lack of automatic firmware updates for smart devices (or no update releases at all), insecure update mechanisms, insecure settings (by default), weak passwords, vulnerabilities in software and web applications, direct network connection to the Internet, insecure authentication methods. Exploitation of vulnerabilities in routers, storage systems, access control and other IoT devices contributes to the spread of malicious software in the IoT infrastructure and compromising IoT devices. The low level of security of IoT devices leads to the fact that a large number of such devices can be compromised with a high degree of probability and used as a means to carry out various attacks both inside and outside the IoT infrastructure. Attacks on IoT infrastructure result in device hacking, data theft, financial loss, instability, or even physical damage to devices. In turn, given the specific nature of these hacked IoT devices, damage to them can lead to injury to people working or dependent on these devices. At the same time, the owners of hacked IoT devices indirectly become accomplices in cyber-crimes. The article provides an overview of known methods for detecting cyber-attacks on the infrastructure of the Internet of things based on machine learning methods. Despite the large number of such approaches, the problem of detecting zero-day cyber-attacks in the IoT infrastructure is still unresolved. This leads to the need to find new approaches that can solve this problem.

Keywords

Internet of Things (IoT), cyberattack, distributed denial of services (DDoS), cyberattack detection, cybersecurity

1. Introduction

The Internet of Things is one of the most versatile technologies that allow innovations to be introduced into various economic sectors and areas of human activity, including critical infrastructure facilities and the industrial Internet of Things. At the same time, the infrastructure of the Internet of things can simultaneously include both devices that are used for office automation and devices for operational technologies. IoT devices in these infrastructures can impact mission-critical systems (such as database servers) through the ability to collect and monitor IoT system data. Even if a smart device is highly specialized or has limited resources to pose a threat, there is always a risk that this

IntelITSIS'2022: 3rd International Workshop on Intelligent Information Technologies and Systems of Information Security, March 23–25, 2022, Khmelnytskyi, Ukraine

EMAIL: bobrovnikova.kira@gmail.com (K. Bobrovnikova); sirogyk@ukr.net (S. Lysenko); devastator167384@gmail.com (I. Hurman); andrzej.kwiecien@polsl.pl (A. Kwiecień)
ORCID: 0000-0002-1046-893X (K. Bobrovnikova); 0000-0001-7243-8747 (S. Lysenko); 0000-0002-2282-3484 (I. Hurman); 0000-0003-1447-3303 (A. Kwiecień)

device will be used to hack into more important components of the IoT infrastructure. The severity and strength of this impact depends on the environment in which insecure IoT devices are installed [1].

Weak or even no security for IoT devices leaves smart devices more vulnerable than servers and computers. This is facilitated by the constant availability of smart devices on the network, the lack of automatic firmware updates for smart devices (or the lack of update releases at all), and the lack of awareness of users about potential cyber security risks.

IoT devices are easily vulnerable to outdated or untrusted components, insecure update mechanisms, insecure default settings, weak passwords, use of insecure network services such as Telnet and SSH, or insecure services (such as web-based management consoles). Security issues in the protocols used in the IoT infrastructure can have a devastating effect on the entire infrastructure. Vulnerabilities in software and web applications can be used to distribute malicious updates and steal credentials.

Thus, the critical components in the infrastructure of the Internet of Things can be both the smart devices themselves and the communication channels and software [2].

2. Cyber Security Risks and Threats to Internet of Things Infrastructure

Cybersecurity risks in IoT infrastructure are exacerbated by a number of key factors inherent in IoT (Figure 1). Although these factors increase the functionality of the IoT infrastructure, at the same time, they are critical from a security point of view [1].

Security issues in the IoT infrastructure also have specific features. For example, an IoT system may consist of groups of identical or similar devices. Device homogeneity amplifies the potential impact of each possible vulnerability by multiplying it by the number of similar devices that have the same characteristics. For example, a vulnerability in a device communication protocol when connected to the Internet of Things could spread to other devices using the same protocol or having an identical design.

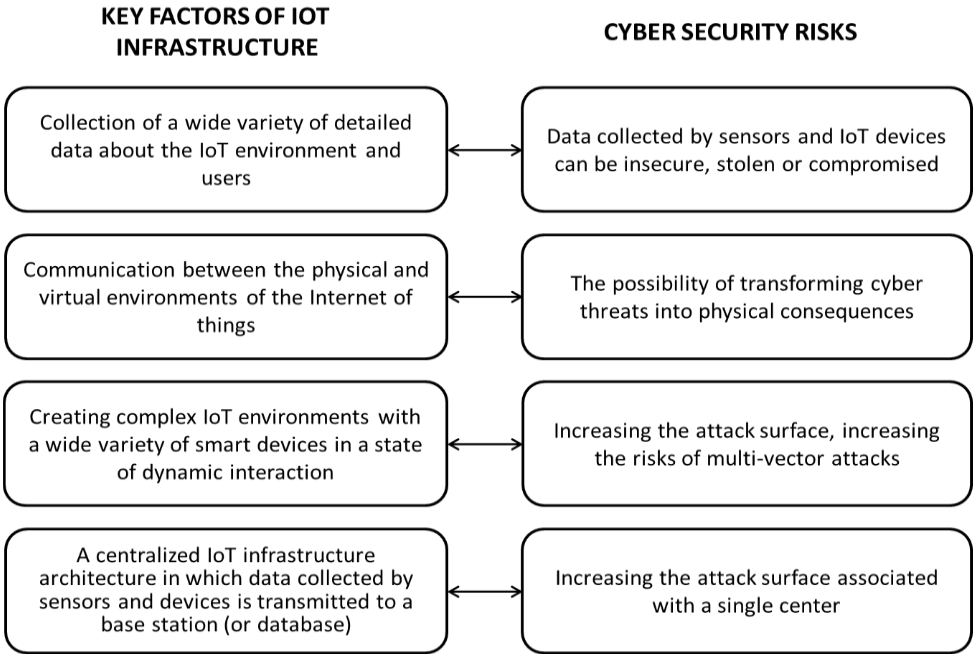
KEY FACTORS OF IOT INFRASTRUCTURE
CYBER SECURITY RISKS
Collection of a wide variety of detailed data about the IoT environment and users
Data collected by sensors and IoT devices can be insecure, stolen or compromised
Communication between the physical and virtual environments of the Internet of things
The possibility of transforming cyber threats into physical consequences
Creating complex IoT environments with a wide variety of smart devices in a state of dynamic interaction
Increasing the attack surface, increasing the risks of multi-vector attacks
A centralized IoT infrastructure architecture in which data collected by sensors and devices is transmitted to a base station (or database)
Increasing the attack surface associated with a single center

Figure 1: Key factors influencing cyber security risks in IoT infrastructure

Deployment of IoT devices can occur under conditions that make it impossible or difficult to further upgrade or reconfigure devices. In addition, IoT devices may be left without manufacturer support in the long run. In such a situation, the security mechanisms in place at the time of deployment may be unusable as new threats emerge in the future. This will introduce new vulnerabilities. Thus, the technical support and management of IoT devices in the long term is a serious security issue.

Another specific IoT security issue is that the user may often be unaware of the internal functioning of an IoT device or the data streams it generates. This creates vulnerability where an IoT device can perform unwanted actions without the user's knowledge, such as collecting data that the user does not intend to provide. The functionality of an IoT device can also change without the user's knowledge through device firmware updates, leaving the user at risk from any changes made by the device manufacturer.

Threats to the IoT infrastructure can be divided into the following categories [3]: spoofing, information disclosure, tampering, elevation of service and Distributed Denial of Service (DDoS) (Figure 2). Attackers typically use these threats as an entry point and then move on to other malicious activities such as stealing data, blocking connections, or infecting devices with ransomware.

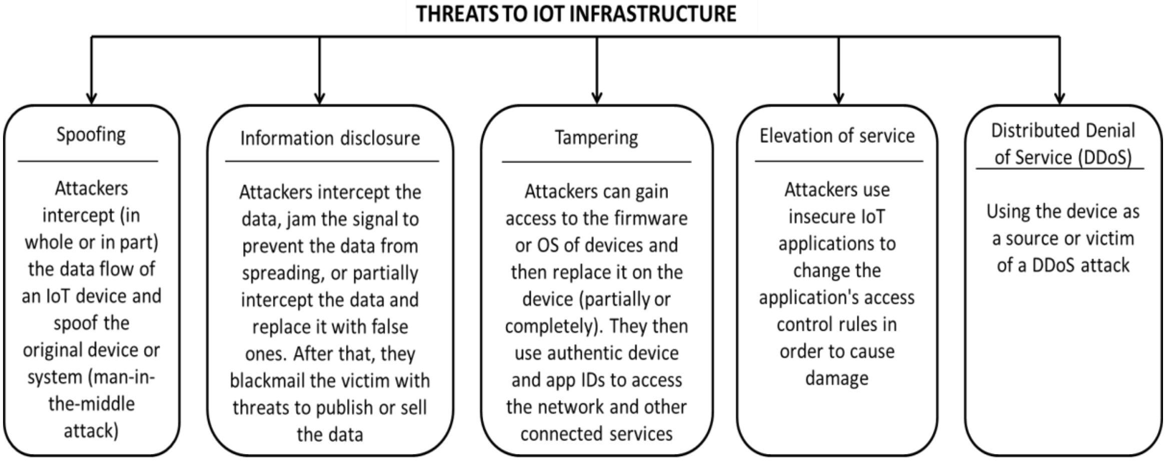
THREATS TO IOT INFRASTRUCTURE
Spoofing
Attackers intercept (in whole or in part) the data flow of an IoT device and spoof the original device or system (man-in-the-middle attack)
Information disclosure
Attackers intercept the data, jam the signal to prevent the data from spreading, or partially intercept the data and replace it with false ones. After that, they blackmail the victim with threats to publish or sell the data
Tampering
Attackers can gain access to the firmware or OS of devices and then replace it on the device (partially or completely). They then use authentic device and app IDs to access the network and other connected services
Elevation of service
Attackers use insecure IoT applications to change the application's access control rules in order to cause damage
Distributed Denial of Service (DDoS)
Using the device as a source or victim of a DDoS attack

Figure 2: Threats to IoT infrastructure

One of the most common threats to IoT infrastructure is a Distributed Denial of Service attack [4, 5]. One of the common goals of DDoS attacks is the task of "putting down" a service, which leads to a loss of profit for the owner. The purpose of this type of attack is often online stores, banks, and gaming services. The duration of such attacks can last from several hours to several days with a powerful amount of traffic that reaches a terabit of data. Attacks on individuals, the purpose of which is to break into home devices and servers, also remain relevant for attackers. However, organizations are most often attacked through smart things, while the number of attacks through home IoT devices has decreased somewhat. Because industrial IoT devices are often isolated from the outside world, these smart devices are less susceptible to attacks. Often, DDoS attacks are not intended to “destroy” important infrastructure components, but serve only as a distraction to hide the real attack. When trying to break into the DDoS infrastructure, the attack is launched in parallel with the true attack [6].

3. Machine Learning-Based Solution for IoT Cyber-Attacks Detection

There are many approaches to solving cybersecurity problems [7, 8], including the detection of cyber-attacks on the infrastructure of the Internet of Things (Table 1). One of the most promising approaches to detect attacks in the field of cybersecurity is algorithms based on machine learning [9-13]. In particular, in the paper [14] an approach based on IoT malware traffic analysis, using multilevel artificial intelligence was proposed. This approach applies a combination of neural network and a binary visualization and learns from the misclassifications to improve its efficiency.

The approach consists of three stages: collection of network traffic; a binary visualization stage in which the collected traffic is stored in ASCII and converted to a 2D image; processing and analysis of this binary image by the TensorFlow module. TensorFlow is an end-to-end open source platform for solving machine learning problems to automatically find and classify patterns. The advantage of the platform is the ease of retraining and the excellent ability of image recognition, including detecting differences that are inaccessible to the human eye. The TensorFlow module is built on top of a CNN, with an additional layer at the beginning called a convolution.

The approach uses an algorithm for visual representation of the collected traffic, based on binary data visualization tool Binvis. Thus, the result of Binvis is the representation of the characteristics of network traffic in the form of an image. The binary output of Binvis is broken into a number of tiles. The TensorFlow machine learning algorithm predicts what each of the tiles represents, and then determines the combination of tiles on which the image is based. This allows parallelizing operations and detecting an object regardless of its location in the image. The proposed technique makes it possible to protect IoT devices on gateway level bypassing the limitations of IoT environment.

The paper [15] presents a deep learning based intrusion detection system (DL-IDS) for IoT infrastructure. According to the proposed approach, in order to detect intrusions into the infrastructure of the Internet of Things based on the analysis of network traffic, the collected traffic is pre-processed to normalize it and eliminate uncertainties in the data set. To replace missing values and eliminate redundancy, the similarity of the data in the dataset is measured using the Minkowski distance. Based on the distance between each data pair, redundant and duplicate data is removed from the dataset and passed to the next preprocessing step. At the next stage, in order to avoid bias of the classification results towards more frequent entries, the missing attribute values in the data set are replaced by the computed values of the nearest neighbor. For this purpose, the K nearest neighbors in Euclidean distance are determined, and the missing values are replaced by the average values for the obtained data. To select the most important traffic features that may indicate the fact of an intrusion into the Internet of Things environment, the spider monkey optimization algorithm (SMO) was used. In order to detect intrusions into the IoT environment, a stacked-deep polynomial network (SDPN) was used to classify incoming data as normal or abnormal. Anomalous data may indicate an intrusion into the IoT environment, such as the presence of a user-to-root (U2R) attack, a remote-to-local (R2L) attack, a denial of service (DoS) attack, a probe attack. In [16] an AD-IoT system for detecting cyber-attacks on fog computing nodes in the smart city infrastructure is proposed. AD-IoT system is based on Random Forest machine learning algorithm and makes it possible to detect compromised IoT devices that are located in distributed fog nodes. The determination of normal and abnormal device behavior is based on the monitoring and analysis of network traffic that passes through each of the fog nodes. If fog level attacks are detected, the system informs the cloud security services about the results obtained and the system updates made. The results of the experiments showed that the proposed system makes it possible to achieve an acceptable accuracy in detecting attacks on the smart city infrastructure. In [17] experimental studies and a comprehensive analysis of twelve different machine learning algorithms were carried out in order to assess the accuracy of detecting anomalous behavior in Internet of Things networks using these algorithms. The results obtained show that for all the applied datasets, the Random Forest algorithm has the best performance in terms of Receiver Operating Characteristic (ROC) curves, Precision, Recall, F1-Score and Accuracy. It is also concluded that other studied machine learning algorithms demonstrate efficiency quite close to Random Forest. The choice of machine learning algorithm depends on the data to be analyzed.

In the work [18] an approach based on the paradigm of software-defined networks (SDN) and cloud technologies is proposed. Decentralized two-layer SDN is used to detect and mitigate DDoS attacks in the wireless IoT environment. The local domain controller of that domain is used to control traffic for each subnet domain. At the same time, a universal controller connected to local controllers is located in the cloud environment. Local controllers collect traffic from their domains and extract many features from it to detect the presence of DDoS attacks in the domain. To detect DDoS attacks, 155 features were used, removed using the SPAN (switched port analyzer) function of the Cisco Nexus switch. Among these features are: frame.time_epoch, frame.interface_id, frame.len, radiotap.length, radiotap.pad, wlan.fc.frag, wlan.frag, wlan.duration, data.len.

The collected features are used by the DDoS detection modules implemented on all local controllers. In order to detect DDoS attacks, an extreme learning machine (ELM), which is a feed-forward neural network, and semi-supervised learning were used. The advantage of using ELM is the reduction of training time by randomly selecting the initial parameters, as well as the use of simple matrix operations. This makes it possible to accelerate retraining and thereby perform real-time detection. A DDoS attacks mitigation module is also deployed on local controllers. The universal controller is used to provide data exchange between local controllers, such as local blacklists generated by local domain controllers. The proposed DDoS mitigation approach defines separate strategies that define different attack mitigation scenarios for mobile and fixed devices in the wireless Internet environment.

The work [19] is devoted to the study of the effectiveness of the use of machine learning classifiers in anomaly-based IDS for the infrastructure of the Internet of things. The efficiency and possibilities of using several single classifiers and their ensembles were investigated. To evaluate the performance of the classifiers, such characteristics as accuracy, error rates, specificity, sensitivity, and areas under the ROC curve were used. In order to conduct a statistical analysis of significant differences for the classifiers, the Nemenya and Friedman tests were applied. The response time of the classifiers was also evaluated when applied in a specific IoT environment as part of the IDS. Based on the performance evaluation and statistical analysis, it was concluded that extreme gradient boosting, regression trees and classification trees are characterized by the most acceptable classification efficiency and response times. In [20] the effectiveness of using several machine learning classifiers to analyze botnet traffic in the IoT environment was analyzed. To this end, datasets for several types of botnet attacks were classified for nine IoT devices. For each of the analyzed classifiers, such characteristics as Accuracy, Precision, Recall, True Positive, True Negative, False Positive, False Negative and F1-score were calculated. The results of the experimental studies have shown that the best results are demonstrated by the use of Random Forest, and the lowest - by the use of Support Vector Machine. At the same time, the obtained rather high F1-scores show the reliability of all three studied classifiers. The disadvantage of the technique is the use of all available features in datasets for analysis. In the article [21] an intelligent system for the IoT cyber-attack detection in the IoT network is presented. The system is based on using a hybrid approach to reduce the set of features. For this purpose, feature ranking on the basis of using correlation coefficient, mean decrease accuracy of random forest and gain ratio is performed. Thus, three different feature sets are formed. The resulting features are then combined using a specially designed technique to obtain an optimized set of features. The resulting feature set was processed by machine learning algorithms such as K-Nearest Neighbor, Random Forest and XGBoost. BoT-IoT, DS2OS and NSL-KDD datasets were used for conducting experiments to evaluate the effectiveness of the approach. The performance of the system was evaluated and compared with some known methods found in the literature in terms of Detection Rate, Accuracy, Precision and F1-score. In [22] a method for detecting DDoS attacks based on hybrid optimization is proposed. The method uses a hybrid Metaheuristic lion optimization algorithm and Firefly optimization algorithm (ML-F). The collected data is pre-processed to remove noise and fill in missing data. Features that may indicate the presence of attacks are extracted from the processed data by applying Recursive feature elimination (RFE). Data separation based on hybrid ML-F optimization algorithm allows selecting low rate attacks. In order to classify attacks, a random forest classifier is used. Using the proposed approach allows us to improve performance compared to the gradient boost classifier algorithm. In the study [23] a Local-Global best Bat Algorithm for Neural Networks (LGBA-NN) to select feature sets and hyperparameters for efficient botnet attacks detection was proposed. For this purpose, 9 commercial IoT devices infected with Gafgyt and Mirai botnets were used.The presented Bat Algorithm (BA) used the local-global best-based inertia weight to update the velocity of bat in the swarm. In the population initialization Gaussian distribution was used to tackle with swarm diversity of algorithm. With purpose to obtain better exploration during each generation, the local search mechanism was followed by the Gaussian density function and local-global best function. Improved algorithm was employed for neural network hyperparameter tuning and weight optimization to classify 10 classes of botnet attacks. The performance of LGBA-NN was compared with other new approaches such as weight optimization using BA-NN and Particle Swarm Optimization (PSO-NN). The experimental results revealed the superiority of the proposed technique (with 90% accuracy) over other techniques, i.e., BA-NN (accuracy of 85.5%) and PSO-NN (accuracy of 85.2%) in botnet attack detection. In the paper [24] architecture for detecting DoS/DDoS attacks in IoT using machine learning methods is presented. The proposed architecture includes DoS/DDoS attack detection and DoS/DDoS mitigation. To detect DoS/DDoS attacks, a multiclass classifier based on the concept of "Looking back" was used. The detection component makes it possible to determine the type of attack and the type of packet used in the attack. This allows appropriate mitigation measures to be taken against attacks using specific packet types.

The work [25] introduces an intrusion detection technique which used an ensemble-based voting classifier that combines multiple classifiers as a base learner. In order to get the final prediction, presented classifier gives the vote to the predictions of the traditional classifier. To evaluate the effectiveness of the proposed technique, experiments are performed on a set of different IoT devices such as fridge sensor, garage door, GPS sensor, modbus, light motion, thermostat and weather. The proposed technique was tested for binary and multi-class attacks classification (such as Password, Scanning, XSS, DDos, Ransomeware, Injection, Backdoor).

The performance of the proposed technique has been compared with the other new intrusion detection algorithms available in the literature. A comparison has been drawn against the matrices of accuracy, precision, recall and F-score with different combinations of Decision Tree, Naive Bayes, Random Forest, and K-Nearest Neighbours machine learning algorithms: DT-RF-kNN-NB, DT-RF-NB, and DT-RF-kNN. The evaluation result showed that the proposed method is more efficient in most cases.

Table 1

Efficiency, data sets and machine learning algorithms of modern techniques to detecting cyber-attacks in the Internet of Things infrastructure

Authors	Year	Goal	Machine Learning methods	Data set	Result
R. Shire, S. Shiaeles, K. Bendiab, B. Ghita & N. Kolokotronis [14]	2019	detection and classification zero-day malware	Convolutional Neural Network and binary visualization	real network environ-ments	Accuracy of 91.32%, Precision of 91.67%, Recall of 91.03%
Y. Otoum, D. Liu & A. Nayak [15]	2019	detection of DoS, user-to-root (U2R), remote-to-local (R2L), probe, intrusions	Stacked-Deep Polynomial Network	NSL-KDD	Accuracy of 99.02%, Precision of 99,4%, Recall of 98,3%, F1-score of 98,8%
I. Alrashdi, A. Alqazzaz, E. Aloufi, R. Alharthi, M. Zohdy & H. Ming [16]	2019	anomaly and attack detection	Random Forest	UNSW-NB15	Precision of 79%, Recall of 97%, F1-score of 86%
N. Elmrabit, F. Zhou, F. Li, & H. Zhou [17]	2020	anomaly and attack detection	Decision Tree, Random Forest, Adaptive boosting, K-Nearest Neighbours, Logistic Regression, Naive Bayes, Simple Recurrent Neural Network, Gated Recurrent Units, Convo-lutional Neural Network and Long short-Term Memory, Convolu-tional Neural Network, Long short-Term Memory, Deep	CICIDS-2017, ICS Cy-berat-tack, UNSW-NB15	Performance at up to 99.9% for Random Forest on CICIDS-2017

Authors	Year	Goal	Machine Learning methods	Data set	Result
Neural Network					
N. Ravi & S. M. Shalinie [18]	2020	DDoS attacks detection and mitigation	Semi-supervised Extreme Learning Machines, ELM	UNB-ISCX	Accuracy up to 96,28%
A. Verma & V. Ranga [19]	2020	research on the effectiveness of using ML classifiers for anomaly detection-based IDS to detect DoS attacks	Classification and Regression Trees, Multilayer Perceptron, Random Forest, Extremely Randomized Trees, AdaBoost, Gradient Boosted Machine, Extreme Gradient Boosting	CIDDS-001, UNSW-NB15, NSL-KDD	Regression Trees, Classification Trees and Extreme Gradient Boosting show the best results - Accuracy of 96.7%, Specificity of 96.2%, Sensitivity of 97.3%, with acceptable response time
S. Bagui, X. Wang & S. Bagui [20]	2021	intrusion detection	Support Vector Machine, Logistic Regression, Random Forest	UCI Machine Learning Repository	Accuracy of 99%
P. Kumar, G. P. Gupta, & R. Tripathi [21]	2021	cyber-attack detection for IoT network	Random Forest, K-Nearest Neighbor, XGBoost	NSL-KDD, BoT-IoT, DS2OS	Accuracy above 99%, Detection Rate up to 90%-100%
E. S. Krishna, A. Thangavelu [22]	2021	DDoS attacks detection	Random Forest	NSL-KDD, NBaIoT	Accuracy of 99.98%, Precision of 99.87%, Recall of 100% and F-score of 99.73%
A. Alharbi, W. Alosaimi, H. Alyami, H. T. Rauf, & R. Damaševičius [23]	2021	DDoS attacks detection	Bat Algorithm	N-BaIoT	Accuracy of 90%
M. A. Khan, M. A. Khan Khattk, S. Latif, A. A. Shah, M. Ur Rehman, W. Boulila, ... & J. Ahmad [24]	2022	intrusion detection	combined Decision Tree, Naive Bayes, Random Forest, and K-Nearest Neighbours using a voting-based technique	TON IoT	Accuracy of 88%, Precision of 90%, Recall of 88%, F-score of 88% for DT-RF-NB with Binary classification on combined IoT dataset
A. Mihoub, O. B. Fredj, O. Cheikhrouhou, A. Derhab & M.	2022	investigation of DoS/DDoS attacks detection for	Looking-Back-enabled Random Forest	IoT-Bot	Accuracy of 99.81%

Authors	Year	Goal	Machine Learning methods	Data set	Result
Krichen [25]		IoT using ML techniques			

Figures 3-6 demonstrate the results of the analyzed cyberattack detection approaches concerning the Internet of Things infrastructure in terms of Accuracy, Recall, Precision and F-score.

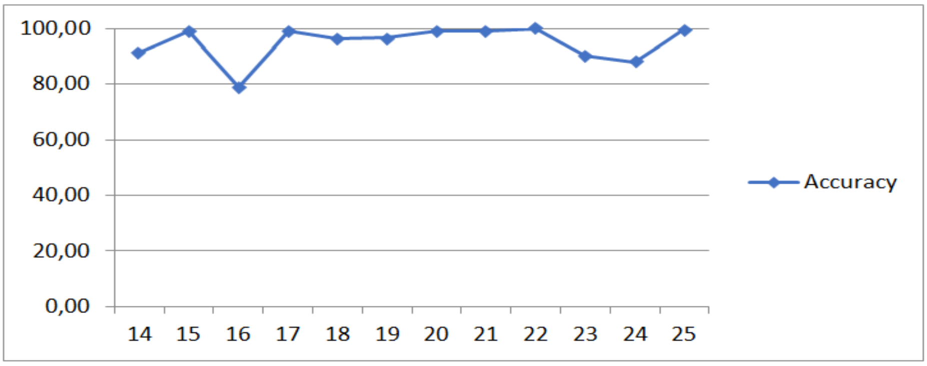

Figure 3: Results of the analyzed cyberattack detection approaches concerning the Internet of Things infrastructure in terms of Accuracy

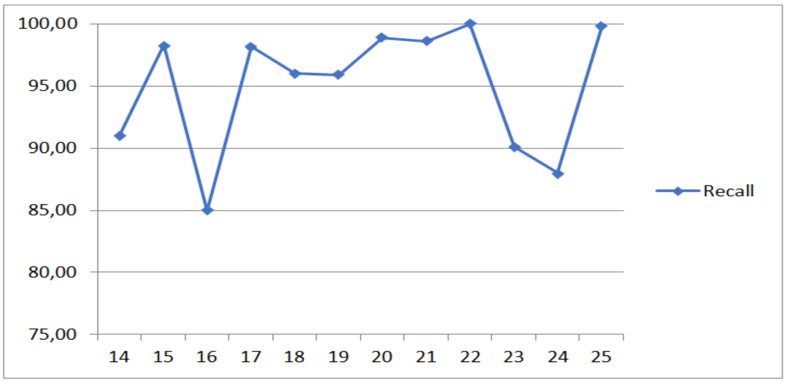

Figure 4: Results of the analyzed cyberattack detection approaches concerning the Internet of Things infrastructure in terms of Recall

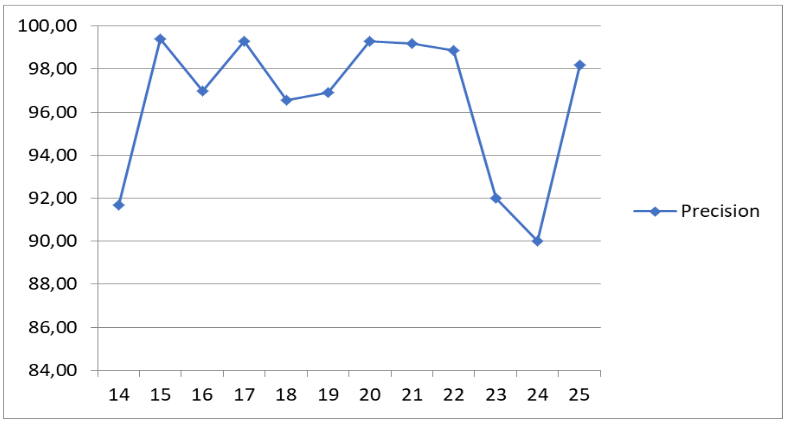

Figure 5: Results of the analyzed cyberattack detection approaches concerning the Internet of Things infrastructure in terms of Precision

4. Conclusions

The paper provides an overview of machine learning approaches to detecting attacks in the IoT infrastructure. Known methods for detecting attacks demonstrate a high level of efficiency, at the same time, they have a number of common limitations and shortcomings, as evidenced by the constant increase in the number of cyber-attacks on the IoT infrastructure. The main disadvantages of known techniques are the inability to detect and adaptively respond to still unknown attacks (zero-day attacks), as well as the low level of detection of multi-vector attacks. In addition, many well-known approaches are characterized by a high level of false positives. A common disadvantage of most of the known approaches is a significant response time, which is unacceptable for real-time systems. Another important disadvantage of the known approaches is the need for significant amounts of computing resources. Also, an important aspect that requires special attention is the selection of a minimum and at the same time sufficient set of informative features that indicate the presence of attacks in the IoT infrastructure. Thus, there is still a need to develop new techniques for detecting attacks in the IoT infrastructure that will take into account the shortcomings of known approaches and improve the accuracy of detecting known and unknown attacks in the IoT infrastructure.

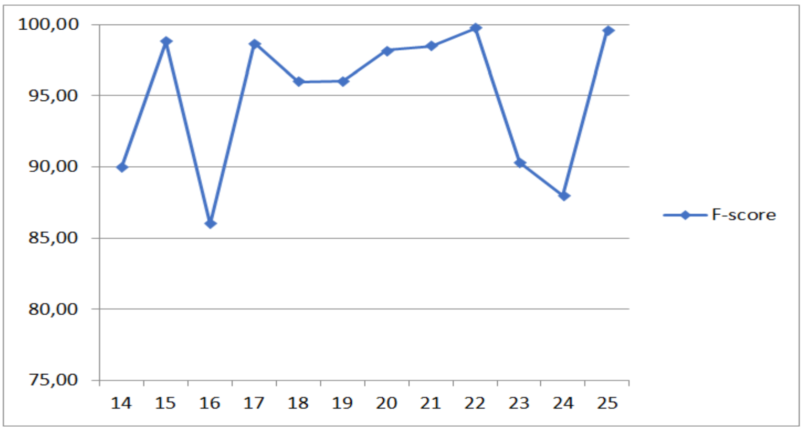

Figure 6: Results of the analyzed cyberattack detection approaches concerning the Internet of Things infrastructure in terms of F-score

5. References

[1] Trend Micro. The IoT Attack Surface: Threats and Security Solutions. URL: https://www.trendmicro.com/vinfo/mx/security/news/internet-of-things/the-iot-attack-surface-threats-and-security-solutions

[2] V. Kharchenko, Y. Ponochovnyi, A. Boyarchuk, & A. S. Qahtan. Security and availability models for smart building automation systems. International Journal of Computing, 2017, 16 (4), pp. 194-202.

[3] Tackle IoT application security threats and vulnerabilities. URL: https://www.techtarget.com/iotagenda/tip/Tackle-IoT-application-security-threats-and-vulnerabilities

[4] K. Singh, K. S. Dhindsa, & B. Bhushan. Performance analysis of agent based distributed defense mechanisms against DDOS attacks. International Journal of Computing, 2018, 17 (1), pp. 15-24.

[5] A. Balyk, M. Karpinski, A. Naglik, G. Shangytbayeva, I. Romanets. Using Graphic Network Simulator 3 for DDoS Attacks Simulation. International Journal of Computing, 2017, 16 (4), pp. 219-225.

[6] 2022 IoT and OT threat landscape assessment report. URL: https://sectrio.com/iot-security-reports/2022-iot-and-ot-threat-landscape-assessment-report/

[7] O. Kehret, A. Walz, A. Sikora. Integration of Hardware Security Modules into a Deeply Embedded TLS Stack. International Journal of Computing, 2016, 15 (1), pp. 24-32.

[8] W. Winiecki, P. Bilski. Implementation of Symmetric Cryptography in Embedded Measurement Systems. International Journal of Computing, 2015, 14 (2), pp. 66-76.

[9] S. Lysenko, O. Pomorova, O. Savenko, A. Kryshchuk and K. Bobrovnikova. DNS-based Anti-evasion Technique for Botnets Detection. Proceedings of the 8-th IEEE International

Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Warsaw (Poland), September 24–26, 2015, pp. 453–458

[10] B. Savenko, S. Lysenko, K. Bobrovnikova, O. Savenko, G. Markowsky. Detection DNS Tunneling Botnets. Proceedings of the 2021 IEEE 11th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Cracow, Poland, September 22-25, 2021, Vol. 1, pp. 64-69. IEEE

[11] S. Lysenko, K. Bobrovnikova, R. Shchuka, O. Savenko. A cyberattacks detection technique based on evolutionary algorithms. In 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), 2020, pp. 127-132. IEEE.

[12] G. Suchacka, J. Iwariski. Identifying legitimate Web users and bots with different traffic profiles - an Information Bottleneck approach. Knowledge-Based Systems, 2020,197, 10587S

[13] T. Sochor, N. Chalupova. Interpersonal Internet Messaging Prospects in Industry 4.0 Era. In: Recent Advances in Soft Computing and Cybernetics. Springer, Cham, 2021. p. 285-295.

[14]R. Shire, S. Shiaeles, K. Bendiab, B. Ghita, N. Kolokotronis. Malware squid: A novel iot malware traffic analysis framework using convolutional neural network and binary visualisation. In Internet of Things, Smart Spaces, and Next Generation Networks and Systems, Springer, Cham, 2019, pp. 65-76.

[15] Y. Otoum, D. Liu & A. Nayak. DL-IDS: a deep learning-based intrusion detection framework for securing IoT. Transactions on Emerging Telecommunications Technologies, 2019, e3803.

[16] I. Alrashdi, A. Alqazzaz, E. Aloufi, R. Alharthi, M. Zohdy & H. Ming. Ad-iot: Anomaly detection of iot cyberattacks in smart city using machine learning. In 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), IEEE, 2019, pp. 0305-0310.

[17] N. Elmrabit, F. Zhou, F. Li, & H. Zhou. Evaluation of machine learning algorithms for anomaly detection. In 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), IEEE, 2020, pp. 1-8.

[18] N. Ravi & S. M. Shalinie. Learning-driven detection and mitigation of DDoS attack in IoT via SDN-cloud architecture. IEEE Internet of Things Journal, 2020, 7(4), pp. 3559-3570.

[19] A. Verma & V. Ranga. Machine learning based intrusion detection systems for IoT applications. Wireless Personal Communications, 2020, 111(4), pp. 2287-2310.

[20] S. Bagui, X. Wang & S. Bagui. Machine Learning Based Intrusion Detection for IoT Botnet. International Journal of Machine Learning and Computing, 2021, 11(6).

[21] P. Kumar, G. P. Gupta, & R. Tripathi. Toward design of an intelligent cyber-attack detection system using hybrid feature reduced approach for IoT networks. Arabian Journal for Science and Engineering, 2021, 46(4), pp. 3749-3778.

[22] E. S. Krishna, A. Thangavelu. Attack detection in IoT devices using hybrid metaheuristic lion optimization algorithm and firefly optimization algorithm. International Journal of System Assurance Engineering and Management, 2021, pp. 1-14.

[23] A. Alharbi, W. Alosaimi, H. Alyami, H. T. Rauf, & R. Damaševičius. Botnet attack detection using local global best bat algorithm for industrial internet of things. Electronics, 10(11), 2021, p.1341.

[24] M. A. Khan, M. A. Khan Khattk, S. Latif, A. A. Shah, M. Ur Rehman, W. Boulila, ... & J. Ahmad. Voting classifier-based intrusion detection for IoT networks. In Advances on Smart and Soft Computing, Springer, Singapore. 2022, pp. 313-328.

[25] A. Mihoub, O. B. Fredj, O. Cheikhrouhou, A. Derhab & M. Krichen. Denial of service attack detection and mitigation for internet of things using looking-back-enabled machine learning techniques. Computers & Electrical Engineering, 2022, 98, p. 107716.

[26] K. Bobrovnikova, S. Lysenko, B. Savenko, P. Gaj, O. Savenko. Technique for IoT malware detection based on control flow graph analysis. Radioelectronic and Computer Systems, 2022(1), pp. 141–153.

[27] IoT dataset. URL: https://github.com/thieu1995 /iot dataset (accessed 10.02.2022).