UDC 004.896
DOI: 10.31891/CSIT-2021-5-15

KIRA BOBROVNIKOVA, MARIIA KAPUSTIAN, DMYTRO DENYSIUK
Khmelnytskyi National University

RESEARCH OF MACHINE LEARNING BASED METHODS FOR CYBERATTACKS DETECTION IN THE INTERNET OF THINGS INFRASTRUCTURE

The growing demand for IoT devices is accelerating the pace of their production. In an effort to accelerate the launch of a new device and reduce its cost, manufacturers often neglect to comply with cybersecurity requirements for these devices. The lack of security updates and transparency regarding the security status of IoT devices, as well as unsafe deployment on the Internet, makes IoT devices the target of cybercrime attacks. Quarterly reports from cybersecurity companies show a low level of security of the Internet of Things infrastructure. Considering the widespread use of IoT devices not only in the private sector but also in objects for various purposes, including critical infrastructure objects, the security of these devices and the IoT infrastructure becomes more important.

Nowadays, there are many different methods of detecting cyberattacks on the Internet of Things infrastructure. Advantages of applying the machine-based methods in comparison with signature analysis are the higher detection accuracy and fewer false positive, the possibility of detecting both anomalies and new features of attacks. However, these methods also have certain disadvantages. Among them there is the need for additional hardware resources and lower data processing speeds. The paper presents an overview of modern methods aimed at detecting cyberattacks and anomalies in the Internet of Things using machine learning methods. The main disadvantages of the known methods are the inability to detect and adaptively respond to zero-day attacks and multi-vector attacks. The latter shortcoming is the most critical, as evidenced by the constantly increasing number of cyber attacks on the Internet of Things infrastructure. A common limitation for most known approaches is the need for significant computing resources and the significant response time of cyberattack detection systems.

Keywords: Internet of Things (IoT), machine learning, anomaly detection, attacks detection, intrusions detection

КІРА БОБРОВНІКОВА, МАРІЯ КАПУСТЯН, ДМИТРО ДЕНИСЮК
Хмельницький національний університет

ДОСЛІДЖЕННЯ МЕТОДІВ ВИЯВЛЕННЯ КІБЕРАТАК В ІНФРАСТРУКТУРІ ІНТЕРНЕТУ РЕЧЕЙ НА ОСНОВІ МАШИННОГО НАВЧАННЯ

Зростаючий попит на пристрої Інтернету речей призводить до прискорення темпів їх виробництва. Прагнучи прискорити випуск нового пристрою на ринок та зменшити його собівартість, виробники дуже часто нехтують дотриманням вимог кібербезпеки стосовно цих пристроїв. Відсутність оновлень безпеки та прозорості щодо стану безпеки пристроїв Інтернету речей, а також небезпечне розгортання в мережі перетворює пристрої Інтернету речей на об'єкт атак кіберзлочинців. Щоквартальні звіти компаній, пов'язаних з забезпеченням кібербезпеки, свідчать про низький рівень безпеки інфраструктури Інтернету речей. Враховуючи широке використання пристроїв Інтернету речей не лише в приватному секторі, а й на об'єктах різного призначення, включаючи об'єкти критичної інфраструктури, безпека цих пристроїв та інфраструктури Інтернету речей набуває важливого значення.

На сьогоднішній день відомо багато різних методів виявлення кібератак на інфраструктуру Інтернету речей. Перевагами застосування методів машинного навчання в порівнянні з сигнатурним аналізом є вища точність виявлення та менша кількість хибних спрацювань, можливість виявлення аномалій та нових ознак атак. Проте ці методи мають і певні недоліки. Серед них – необхідність в додаткових апаратних ресурсах та більш низька швидкість обробки даних. В роботі представлено огляд сучасних методів, спрямованих на виявлення кібератак та аномалій в мережах Інтернету речей із застосуванням методів машинного навчання. Основними недоліками відомих методів є неспроможність виявлення та адаптивного реагування на атаки нульового дня та мультивекторні атаки. Останній недолік є найбільш критичним, про що свідчить постійне зростання кількості кібератак на інфраструктуру Інтернету речей. Загальним обмеженням для більшості відомих підходів є потреба в значних обсягах обчислювальних ресурсів та значний час відгуку систем виявлення кібератак.

Ключові слова: Інтернет речей (IoT), машинне навчання, виявлення аномалій, виявлення атак, виявлення вторгнень

Introduction

The Internet of Things (IoT) is an integral part of modern society. IoT infrastructure is becoming an integral part of modern cities infrastructure. Virtual infrastructure everywhere controls physical objects for various purposes, including critical infrastructure: from private homes and facilities for various purposes, including manufacturing, to highways, dams and power plants.

Today, the Internet of Things is a loosely interconnected network of physical objects, each of which is deployed to solve specific problems. The physical objects of the Internet of Things contain built-in technologies that allow you to interact with the external environment, transmit data about your condition, and receive data from the outside. Thus, the IoT infrastructure consists of a data network between multiple physical devices that are equipped with built-in tools and technologies to interact automatically with each other and / or with the external environment (such as sensors and actuators), as well as software. Both wired and wireless technologies can be used to connect IoT devices, enabling the transmission and exchange of data between the external environment and other IoT devices using standard communication protocols.

The growing demand for a variety of IoT devices for home automation, smart city infrastructure, medicine and agriculture is accelerating their production. These devices provide new services and enable autonomous support of operation and communications in various industries.

Security issues in the Internet of Things

In an effort to launch a new device as soon as possible and reduce its cost, manufacturers very often develop these devices without taking into account the latest cybersecurity requirements, simplifying or not implementing any security and protection functions at all. Other critical factors are the lack of security updates for IoT devices, the lack of transparency about their security status, and the dangerous deployment with the ability to directly access IoT devices over the Internet. All this turns the Internet of Things devices into the weakest link, which opens up opportunities for hacking and compromising the protected network infrastructure. This, in turn, leads to cyber attacks even in those areas that previously did not pose risks to cybersecurity [1, 2]. In addition, smart IoT devices that regularly collect and use confidential information about their owners, are becoming widespread. This also makes them a desirable target for cybercriminals.

Vulnerable links in the Internet of Things infrastructure can be both Internet of Things devices, which are usually the main means of initiating attacks, and channels that connect the components of the Internet of Things infrastructure with each other [3]. Unprotected by default settings of IoT devices and outdated components, incorrect configuration of these devices, as well as protocols used in the IoT infrastructure [4] can be vulnerable to cyberattacks [4]. Vulnerabilities in web applications and IoT software can allow cybercriminals to compromise systems to send malicious updates or steal user credentials.

Many IoT networks already have compromised or vulnerable IoT devices that can be targeted by various cyberattacks, or that can themselves be the source of a cyberattack on other devices on the Internet. In this case, cyber attacks on the infrastructure of the Internet of Things can be aimed at both privacy and the availability or productivity of the Internet of Things. Thus, any household smart device, such as a coffee machine, can be compromised and used as a source of cyber attack, which will allow cybercriminals to influence critical network systems by monitoring IoT systems and collecting data in the compromised network [1].

Hundreds of thousands of individual unsecured IoT devices, each with low computing power, can be infected by malicious software and criminalized into a single malicious network. A constant connection to the Internet and a low level or complete absence of security features make unsecured IoT devices a convenient tool for organizing powerful cyberattacks. Networks of infected devices are most often used to organize powerful DDoS attacks or as VPN exit nodes. The amount of DDoS traffic generated by the network of infected IoT devices is usually much more powerful than the amount of traffic of malicious networks formed from personal computers [5, 6].

Another way to use infected IoT devices is cryptomining. The limited battery capacity of smartphones does not allow the use of such infected devices for monetization, so infected smart TVs, set-top boxes, etc. are most often used for this purpose. However, any smart IoT devices connected to the Internet, such as water, electricity and gas meters, could potentially be of interest to cybercriminals. The motivation of cybercriminals to carry out attacks can vary: entertainment, theft of confidential information or information that is a trade secret, revenge, extortion or blackmail for financial gain, or even terrorist acts for political or other purposes.

According to the Groupe Speciale Mobile Association [7], the number of Internet of Things devices used worldwide will reach almost 25 billion by 2025 (twice the number of connected devices today). This will increase the risk of cyberattacks targeting these devices. Another important problem today is the impossibility of installing any protective or monitoring solutions on the Internet of Things device, which makes it difficult to prevent malicious activity in the infrastructure of the Internet of Things. Given the rapid integration of the Internet of Things through the Internet of Things platform into various areas of human activity, including critical infrastructure, protecting the Internet of Things infrastructure from cyberattacks is important.

Machine Learning based methods for cyberattacks detection in the Internet of Things infrastructure

Nowadays, there are many approaches to detect cyberattacks in the infrastructure of the Internet of Things, and one of the promising areas are methods based on machine learning (Table 1).

The method proposed in [8] uses cloud technologies and the paradigm of software-defined networks (SDN) to detect and mitigate DDoS-attacks in wireless networks of the Internet of Things (Table 1). This approach uses a two-tier decentralized SDN. Each subnet domain contains a local controller, and in the cloud environment there is a universal controller connected to local controllers. All network traffic is monitored by local controllers, which collect traffic and extract from it a set of features that may indicate the presence of DDoS attacks. For this purpose, 155 features extracted using the switched port analyzer (SPAN) function of the Cisco Nexus switch were used, for example: frame.interface_id, frame.time_epoch, frame.len, radiotap.pad, radiotap.length, wlan.fc.frag, wlan.duration, wlan.frag, data.len. The features removed from the traffic are used for the DDoS detection module, which works on all local controllers. The DDoS mitigation module is also deployed in local controllers. In order to mitigate DDoS attacks, separate strategies have been proposed for mobile and stationary wireless IoT devices.

In order to detect DDoS-attacks, partial learning and an extreme learning machine, ELM - neural network of direct propagation were used. The peculiarity of the extreme learning machines operation is the selection of initial parameters at random and the inclusion of simple matrix operations, which makes it possible to reduce training time. Thus, extreme learning machines can be used in real time, as any retraining will be fairly fast and will not disrupt applications.

In [10] the system of detection of intrusions into the infrastructure of the Internet of Things on the basis of deep learning (DL-IDS) is presented. According to the proposed approach, the traffic of the Internet of Things environment is pre-processed to eliminate uncertainties and normalize the data set, which is to eliminate redundancy and replace missing values. For this purpose, the data similarity in the data set is measured using the Minkowski distance to calculate the distance between each data pair, after which duplicate and redundant data are removed from the data set and transferred to the next pre-processing stage. At the next stage, the missing attribute values in the data are replaced by the calculated values of the nearest neighbor to avoid shifting the classification result towards more frequent records. For this purpose, K nearest neighbors are determined by the Euclidean distance, and the missing value is replaced by the average value for the obtained data.

In order to select the most important signs of traffic that may indicate the fact of intrusion into the Internet of Things, the spider monkey optimization algorithm (SMO) was used. In order to detect intrusions, a stacked-deep polynomial network (SDPN) was used. That makes it possible to classify the input data as normal or abnormal. Abnormal data may indicate an intrusion, such as a denial-of-service (DoS) attack, a user-to-root (U2R) attack, a probe attack, and a remote-to-local (R2L) attack.

In [11] a comprehensive study of the effectiveness and prospects of using classifiers based on machine learning for anomaly-based intrusion detection systems (IDS) in the Internet of Things infrastructure. The most common and dangerous type of attack, the Denial of Service (DoS) attack, was chosen as the main attack for the analysis. The effectiveness of both ensembles of classifiers and single classifiers was analyzed (Table 1). For this purpose, popular data sets were used (Table 1).

Performance of all classifiers was measured in terms of accuracy, specificity, sensitivity, frequency of false positives and the area under the receiver performance curve. Friedman and Nemena tests were used for statistical analysis of significant differences between the studied classifiers. In addition, the response time of classifiers on special IoT equipment was analyzed and the methodology for selecting the best classifier in accordance with the requirements of the intrusion detection system was discussed. Based on the obtained performance results and statistical tests, it was concluded that classifiers such as classification trees, regression trees, as well as extreme gradient boosting show the best compromise between the analyzed classification performance indicators and response time, so it is an acceptable choice for creation of IDS for the IoT environment on the basis of anomalies (Table 1).

In [14], a framework for detecting traffic attacks on the Internet of Things was proposed. The method includes four steps: (1) a new CorrAUC approach to select features that provide sufficient information to detect attack traffic; (2) based on CorrAUC, a new Corrauc feature selection algorithm is developed, which is based on the wrapper technique to accurately filter the most efficient features for the selected machine learning algorithm and consists of Correlation Attribute Evaluation (CAE) and combined with Area Under Roc Curve metrics (AUC); (3) application of the integrated method of multi-criteria decision analysis TOPSIS (Technique for Order of Preference by Similarity to Ideal Solution, multi-criteria decision analysis method) and Shannon Entropy; (4) creating a bijective soft set for testing the selected features to identify IoT attack traffic. The effectiveness of the proposed approach was evaluated using four machine learning algorithms (Table 1). Analysis of experimental results showed that the proposed method can achieve an average of more than 96% efficiency for different machine learning algorithms (Table 1).

[16] proposed an AD-IoT system for detecting cyberattacks on foggy nodes in a smart city infrastructure, based on the Random Forest machine learning algorithm. The proposed solution can effectively detect compromised IoT devices in distributed fog nodes. According to this approach, in order to determine normal and abnormal behavior, network traffic that passes through each foggy node is monitored. Once fog-level attacks are detected, the system should notify the cloud security services of the system analysis and update. The results of the experiments showed that AD-IoT provides an opportunity to achieve acceptable results for detecting attacks (Table 1).

[17] presents a framework for detecting and protecting against abnormal activity in wireless sensor networks IoT (Wireless sensor networks, WSN). It is noted that the formation of botnets is influenced by infrastructure-specific features of the IoT, such as insufficient computing power, power limitations and high density of IoT nodes. Two types of the most common attacks on the Internet of Things device were analyzed. The first type is Bashlite attacks, which target Linux frameworks that transmit data over open telnet. The second type is Mirai attacks, which are aimed at finding vulnerabilities in IoT gadgets that can be attacked through their IP and Mac addresses, after which malicious software is downloaded to hacked devices. A system for detection and protection against abnormal activity is proposed. Three standard sets of benign (normal) data and (abnormal or malicious) data collected from three IoT devices were used as data to analyze these two types of attacks (Table 1). The data used for the analysis is considered as big data. Thus, the processing of these data has the following problems: a large amount of data, its diversity and unstructuredness, lack of data and the need for high-performance processing. Therefore, when pre-processing such data, duplicate data is excluded, after which the minimum, maximum, average and standard deviation of the values of each attribute are calculated. After scaling the data, characteristics in the range from 0 to 1 were obtained. In order to assess the correlation of features and the level of their dependence, the Pearson coefficient was used. WEKA software was used to analyze the obtained data set, and four classifiers were used as machine learning methods (Table 1). Experimental results have shown that the combination of Random Forest and Decision Tree algorithms can provide a fairly high level of accuracy in detecting anomalies and attacks on the Internet of Things.

Table 1

Efficiency, used machine learning methods and sources of modern methods data set for detecting cyberattacks in the infrastructure of the Internet of Things

Authors	Year	Goal	Applied methods	Multiple data	Result
Ravi, N., Shalinie, S. M. [8]	2020	Detection and mitigation of DDoS-attacks	Extreme learning machines, ELM with partial training	UNB-ISCX [9]	Detection accuracy of DDoS-attacks at the level Accuracy (96,28%)
Otoum, Y., Liu, D., Nayak, A. [10]	2019	Detection of DoS type intrusions, user-to-root (U2R), probe, remote-to-local (R2L)	Stacked-deep polynomial network	NSL-KDD [9]	Detection accuracy at the level Accuracy (99.02%), Precision (0.9938), Recall (0.9829), F1-score (0.9883)
Verma, A., Ranga, V. [11]	2020	Research of performance and prospects of use of classifiers based on machine learning for IDS on the basis of anomalies on an example of detection of DoS-attacks	Ensembles of classifiers: Random Forest, AdaBoost, Gradient Boosted Machine, Extreme Gradient Boosting, Extremely Randomized Trees; single classifiers: Classification and Regression Trees, Multi-layer Perceptron	CIDDS-001 [12], UNSW-NB15 [13], NSL-KDD [9]	Classification Trees, Regression Trees, and Extreme Gradient Boosting show the best result with Accuracy up to 96.7%, Specificity up to 96.2%, Sensitivity up to 97.3%, and acceptable response time
Shafiq, M., Tian, Z., Bashir, A. K., Du, X., Guizani, M. [14]	2020	Detection of traffic attacks	Decision Tree (C4.5), Support Vector Machine, Naive Bayes, Random Forest	Bot-IoT Data Set [15]	For Decision Tree C4.5 and Random Forest Specificity is 98,95% and 99,99% respectively, for Naive Bayes and SVM – 98,44% and 98,48% respectively
Alrashdi, I., Alqazzaz, A., Aloufi, E., Alharthi, R., Zohdy, M., Ming, H. [16]	2019	Detection of anomalies and attacks	Random Forest	UNSW-NB15 [13]	Detection of anomalies on the level: Precision – 0.79, Recall – 0.97, F1-score – 0.86
Aysa, M. H., Ibrahim, A. A., Mohammed, A. H. [17]	2020	Detection of anomalies and attacks on the IoT device	Decision Tree (J-48), Linear Support Vector Machine, Neural Network (Back-propagation), Random Forest	Normal and abnormal data collected from the Internet of Things devices, with UCI Machine Learning Repository [18]	Combination of Random Forest and Decision Tree algorithms can provide a high level of Accuracy
Bagui, S., Wang, X., Bagui, S. [19]	2021	Detection of intrusions	Logistic Regression, Random Forest, Support Vector Machine	UCI Machine Learning Repository [18]	Achieved high detection accuracy (about 99%)
Elmrabit, N., Zhou, F., Li, F., Zhou, H. [20]	2020	Detection of abnormal activity, which may indicate the presence of attacks	Logistic Regression, Naive Bayes, Decision tree, Simple Recurrent Neural Network, Gated Recurrent Units, Convolutional Neural Network and Long short-Term Memory, Convolutional Neural Network, Long short-Term Memory, Random Forest, Adaptive boosting, Deep Neural Network, K-nearest Neighbours	CICIDS-2017 [21], UNSW-NB15 [13], ICS Cyberattack [22]	Random Forest (RF) algorithm provides better performance of up to 99.9% for CICIDS-2017
Liu, Z., Thapa, N., Shaver, A., Roy, K., Yuan, X., Khorsandroo, S. [23]	2020	Improving the security of the Internet of Things by applying multiple machine learning techniques to an IoT intrusion dataset	Logistic Regression, Support Vector Machine, K-nearest Neighbours, Random Forest, Extreme Gradient Boosting	IoT Network Intrusion Dataset [24]	Accuracy at 99% using K-nearest Neighbors, while the classification execution time averages 2 minutes. Accuracy at 97% when using Extreme Gradient Boosting, classification execution time – 10,8 sec.

In [19], the traffic of botnets in the IoT environment was analyzed using three classifiers of machine learning (Table 1). Data was classified for each attack on each botnet for nine devices. Indicators such as Accuracy, True Positive, False Positive, False Negative, True Negative, Precision, Recall, F1-score were calculated for each classifier. According to experimental studies, although high detection accuracy (about 99%) was achieved, in general, the use of Random Forest as a classifier gives the best results, and the use of Support Vector Machine - the lowest. However, the obtained high F1-scores demonstrate the reliability of all three classifiers. The disadvantage of this approach is that all available features in the data sets were used for analysis.

In [20], a study of twelve machine learning algorithms in terms of their ability to detect abnormal behavior on the Internet of Things. The assessment is performed on three publicly available data sets (Table 1). Experimental studies were conducted using the ALICE high-performance computing facility at the University of Leicester. On the basis of the conducted experimental researches the complex analysis of application of machine learning algorithms for detection of anomalous behavior in networks of the Internet of things is carried out. The evaluation results confirm that the Random Forest algorithm achieves the best performance in terms of Accuracy, Precision, Recall, F1-Score and Receiver Operating Characteristic (ROC) curves for all applied datasets. It is noted that other machine learning algorithms work with close efficiency to Random Forest, and that the decision on the choice of machine learning algorithm depends on the data to be analyzed.

In [23] the system of intrusion detection on the basis of anomalies is presented. The performance of application of various machine learning algorithms for detection of anomalies in the used set of data on intrusion into the Internet of things in real time is also investigated (Table 1). The experiments showed the highest classification accuracy for K-nearest Neighbors (Table 1). It is noted that one of the important security issues on the Internet of Things is that most of these devices have limited power and computing power. Therefore, encryption and authentication are difficult to use to protect against cyberattacks. Based on this, the detection of network intrusions based on anomalies plays an important role in protecting the Internet of Things from various harmful actions. The advantage of the approach is that when a zero-day attack occurs, the attack signature will not be recognized, but further network behavior will deviate from normal traffic patterns, allowing IDS to detect the anomaly.

Conclusions

A review of cybersecurity companies' reports and antivirus software vendors, as well as literature sources, shows that the problem of detecting cyber attacks in the Internet of Things infrastructure is extremely relevant. The paper provides a brief overview of approaches to detecting attacks in the Internet of Things infrastructure based on machine learning. Although the known methods show a high level of efficiency, nevertheless they have common disadvantages and limitations. The main disadvantages of the known methods are the high level of false positives, the inability to detect and respond to zero-day attacks and multi-vector attacks. The latter shortcoming is the most critical, as evidenced by the steady increase in cyber attacks on the Internet of Things infrastructure. A common limitation for most known approaches is the need for significant amounts of computing resources and significant response time of detection systems, which is unacceptable for real-time operation. Thus, there is still a need to develop new methods of detecting attacks in the Internet of Things infrastructure that would address the shortcomings of known approaches and enable the detection and adaptive response to as yet unknown threats, such as zero-day attacks and multi-vector attacks.

References

1. Trend Micro. Inside the Smart Home: IoT Device Threats and Attack Scenarios. URL: https://www.trendmicro.com/vinfo/it/security/news/internet-of-things/inside-the-smart-home-iot-device-threats-and-attack-scenarios (accessed on November 1, 2021).
2. Check point software technologies LTD. Cyber security report 2021. URL: https://www.checkpoint.com/pages/cyber-security-report-2021/ (accessed on November 1, 2021).
3. OWASP Internet of Things. URL: https://owasp.org/www-project-internet-of-things/#tab=IoT_Attack_Surface_Areas (accessed on November 1, 2021).
4. Nozomi Networks Labs. What IT Needs to Know about OT/IoT Security Threats in 2020. URL: https://www.nozominetworks.com/blog/what-it-needs-to-know-about-ot-io-security-threats-in-2020/ (accessed on November 1, 2021).
5. McAfee Labs Threats Report. URL: https://www.mcafee.com/enterprise/en-us/lp/threats-reports/oct-2021.html (accessed on November 1, 2021).
6. Securelist. New trends in the world of IoT threats. URL: https://securelist.com/new-trends-in-the-world-of-iot-threats/87991/ (accessed on November 1, 2021).
7. Global System for Mobile Communications. URL: https://www.gsma.com/ (accessed on November 1, 2021).
8. Ravi, N., & Shalinie, S. M. 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.
9. UNB. Canadian Institute for Cybersecurity. Datasets. URL: https://www.unb.ca/cic/datasets/index.html (accessed on November 1, 2021).
10. Otoum, Y., Liu, D., & Nayak, A. DL-IDS: a deep learning-based intrusion detection framework for securing IoT. Transactions on Emerging Telecommunications Technologies, 2019, e3803.
11. Verma, A., & Ranga, V. Machine learning based intrusion detection systems for IoT applications. Wireless Personal Communications, 2020, 111(4), pp. 2287-2310.
12. Hochschule Coburg. CIDDS – Coburg Intrusion Detection Data Sets. URL: https://www.hs-coburg.de/forschung/forschungsprojekte-oeffentlich/informationstechnologie/cidds-coburg-intrusion-detection-data-sets.html (accessed on November 1, 2021).
13. UNSW Sydney. The UNSW-NB15 Dataset. URL: https://research.unsw.edu.au/projects/unsw-nb15-dataset (accessed on November 1, 2021).

14. Shafiq, M., Tian, Z., Bashir, A. K., Du, X., & Guizani, M. Corrauc: a malicious bot-iot traffic detection method in iot network using machine learning techniques. IEEE Internet of Things Journal, 2020.

15. UNSW Sydney. Bot-IoT Data Set. https://research.unsw.edu.au/projects/bot-iot-dataset (accessed on November 1, 2021).

16. Alrashdi, I., Alqazzaz, A., Aloufi, E., Alharthi, R., Zohdy, M., & Ming, H. 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. Aysa, M. H., Ibrahim, A. A., & Mohammed, A. H. IoT ddos attack detection using machine learning. In 2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), IEEE, 2020, pp. 1-7.

18. UCI Machine Learning Repository. URL: https://archive.ics.uci.edu/ml/datasets.php (accessed on November 1, 2021).

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

20. Elmrabit, N., Zhou, F., Li, F., & Zhou, H. 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.

21. UNB. Canadian Institute for Cybersecurity. Intrusion Detection Evaluation Dataset (CIC-IDS2017). URL: https://www.unb.ca/cic/datasets/ids-2017.html (accessed on November 1, 2021).

22. Industrial Control System (ICS) Cyber Attack Datasets. URL; ttps://sites.google.com/a/uah.edu/tommy-morris-uah/ics-data-sets (accessed on November 1, 2021).

23. Liu, Z., Thapa, N., Shaver, A., Roy, K., Yuan, X., & Khorsandroo, S. Anomaly detection on iot network intrusion using machine learning. In 2020 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD), IEEE, 2020, pp. 1-5.

24. IEEE DataPort. IoT network intrusion dataset. URL: https://ieee-dataport.org/open-access/iot-network-intrusion-dataset (accessed on November 1, 2021).