Journal of Information Technology and Computing
https://jitc.sabapub.com
ISSN: 2709-5916

2023 Volume 4, Issue 2 : 31 – 38
DOI : 10.48185/jitc.v4i2.890

A SURVEY ON PROMISING DATASETS AND RECENT MACHINE LEARNING APPROACHES FOR THE CLASSIFICATION OF ATTACKS IN INTERNET OF THINGS

Adeniyi U. A.[1], Oyelakin A. M.[2,*]

[1]ICT Centre Air Force Institute of Technology, Kaduna, Nigeria
[2]Department of Computer Science, College of Information and Communication Technology, Crescent University, Abeokuta, Nigeria

Received: 04.11.2023 • Accepted: 20.12.2023 • Published: 30.12.2023 • Final Version: 30.12.2023

Abstract: Securing Internet of Things (IoT) against attacks is a very interesting area of research. A cyberattack refers to as any form of malicious activity that targets IT systems, networks and/or people with a view to gaining illegal access to systems and data they contain. Attacks are in various forms as found in computer systems, networks and the cyber space. The immense increment in the amount of internet applications and the appearance of modern networks has created the need for improved security mechanisms. A good example of such modern technology is Internet of Things (IoTs). An IoT is a system that uses the Internet to facilitate communication between sensors and devices. Several approaches have been used to build attacks detection system in the past. The approaches for classifying attacks have been categorised as signature-based and Machine learning based. However, ML techniques have been argued to be more efficient for the identification of attacks or intrusions when compared to signature-based approaches. This study sourced for relevant literature from notable repositories and then surveyed some of the recent datasets that are very promising for ML-based studies in attack classification in IoT environments. The study equally provided a survey of evolving ML-based techniques for the classification of attacks in IoT networks. The study provided clear directions to researchers working in this area of researches by making the necessary information available more easily for the researcher to go about achieving improved ML-based approaches in this area.

Keywords: Internet of Things, Attacks in IoT, Model Performance, Intrusion Classification Datasets

1. Introduction

Cyber attacks are in various forms due to the threats that are pervasive in networks and the cyber space (Ibitoye, Shafiq & Matrawy, 2019). It has been pointed out that the highest number of monthly attacks was detected in June 2022, with approximately 13 million attacks (Statista, 2023). Similarly, Hussain et al. (2020) argued that network attacks are increasing both in frequency and intensity as of internet of things (IoT) devices are geometrically growing. In recent time, machine learning (ML) algorithms are have been argued to be very popular for classifying attacks in network (Pektas et al., 2018; Oyelakin et al., 2020). Among the networks that have been reported to suffer from different types of attacks is the Internet of Things (IoT) network. The Internet of Things (IoT) constitutes a range of devices, including, but not limited to, IP cameras, smart vehicles, surveillance technologies,

[*] Corresponding Author: moruff.oyelakin@cuab.edu.ng

and wearable devices (Alatram et al., 2023). It is equally regarded as a network of connected devices that can link without human involvement, thanks to the enormous growth in the number of online applications and the development of contemporary technology. IoT enables a large number of items with sensors (including bicycles, coffee makers, lights, and many more items). Also, it has been said that IoT applications are transforming our work and lives by connecting to the internet in sectors such as healthcare, agriculture, transportation, etc. Additionally, it offers countless benefits and countless chances for the sharing of knowledge, innovation, and progress (Alsamiri & Alsubhi, 2019). Tasnim, Hossain, Tabassum and Parvin (2022) pointed out that IoT technology can collect, analyse, and comprehend data about the environment, allowing for modernizations that raise living standards. By making new types of communication between machines and people simpler, smart cities can be created.

In the modern world, IoT technology is used in a variety of ways and scenarios. Everything has become intelligent, including entry doors, window blinds, watches, TVs, fans, light bulbs, and refrigerators. The amount of device engagement is growing daily. Their reliance is increasing as a result. Attackers may not directly hack the target system, but they can easily alter the behaviour of other interdependent devices or the surrounding environment to achieve their objectives. These IoT devices employ a variety of complex encryption and authentication techniques, which consume excessive processing power and result in a noticeable delay, impairing normal operation and lowering performance, especially for real-time IoT devices. For this reason, it is easy for attackers to compromise these devices by taking advantage of memory flaw (Tasnim et al., 2022)

Large-scale distributed denial-of-service (DDoS) assaults on internet-scale infrastructures have been reported in recent years. A continual danger to the ever-expanding IoT world, new botnets like Hajime and Reaper demonstrate how adversaries are always changing their tactics to avoid detection. These IoT-based botnets can swiftly develop into a potent collection of weapons to seriously harm a number of stakeholders. They also exploit a manufacturer's default settings to scan the Internet for other devices (Shaikh, Bou-Harb, Crichigno, & Ghani, 2018).

IoT nodes are unlike other traditional networks in that they lack manual controls, have minimal capacity, and few resources. Additionally, IoT security challenges are becoming increasingly problematic due to the widespread use and rapid proliferation of IoT devices in daily life, necessitating the creation of network-based security solutions. While the existing methods do a good job of detecting some threats, it is still difficult to find others. There is no doubt that there is room for more advanced techniques to improve network security as network attacks rise in number and the amount of information present in networks multiplies dramatically (Alsamiri et al., 2019). Unauthorized individuals may take advantage of a network vulnerability in order to obtain sensitive data and harm the network (Alladi, Chamola, Sikdar & Choo., 2020). This study focuses on building ML-based algorithms for classifying attacks in internet of things. The choosing algorithms are: Random Forest and Adaboost learning algorithms. The study focuses on how to achieve improved ensemble based attacks classification models in Internet of Things environment.

Internet of Things (IoT) is the term used to describe how various entities of an object will communicate with one another in the future. (Jyoti et al., 2017). Saad and Siddeeq (2021) described IoT has one of the technologies that is expanding the fastest right now. It is a technology that enables billions of intelligent objects—referred to as "Things"—to gather various types of data about themselves and their surroundings using a variety of sensors. They can then share this data with the appropriate parties for a variety of purposes, such as controlling and monitoring industrial services, health provision or enhancing business services or functions.

2. Methodology

The methodology used in this study involves souring for relevant literature on promising datasets that can be used for ML-based attack classification in IoT environment as well as different ML-based approaches that have been proposed for attack classification. The researchers established a set of criteria for inclusion of the relevant datasets and articles on IoT security. Each of these datasets was explored and their basic characteristics were discussed. The information were sourced from some of the notable research repositories such as Hindawi, Springer, Elsevier, Google scholar, Science Direct, researchgate.net and many others. The keywords used for the search include: ("datasets for IoT security" AND "datasets for intrusions in IoT" AND "datasets for IoT security") OR ("machine learning for intrusion classification in IoT", OR "attack classification in IoT", OR "IoT intrusions", OR"Machine learning-based Intrusion Detection in IoT environment" OR attack classifications in IoT). The concepts and techniques found in some of the works are then reported as structured in this paper.

Methodological Flow of the Survey

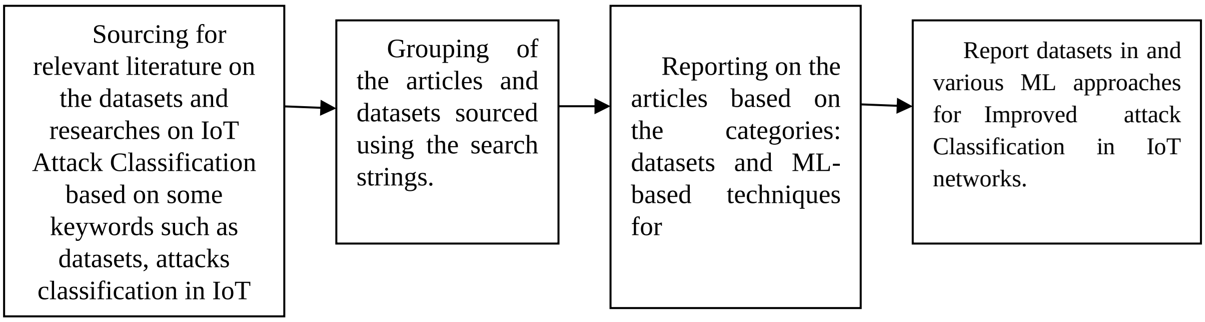
Sourcing for relevant literature on the datasets and researches on IoT Attack Classification based on some keywords such as datasets, attacks classification in IoT
Grouping of the articles and datasets sourced using the search strings.
Reporting on the articles based on the categories: datasets and ML-based techniques for
Report datasets in and various ML approaches for Improved attack Classification in IoT networks.

Figure 1. Flow of the processes in the Study

Figure 1 was used to give a pictorial representation of how the survey of the relevant articles is carried out in this study.

3. A Survey On Datasets For Attack Classification In IoT Networks

Alaram et al. (2023) released a dataset on IoT security recently. The dataset is named DoS/DDoS-MQTT-IoT. It contains different kinds of attacks that can be classified using a ML approach. Another popular dataset is CAIDA dataset. which was released in 2007. This dataset contains approximately one hour of anonymized traffic traces from a DDoS attack on August 4, 2007. Apart from this, a dataset called IOT Security was also released in 2018 (Bezerra et al., 2018). The dataset is terme IoT host-based datasets for intrusion detection research. Another security dataset that is based on IoT investigation is named MedBIoT. The title of the work was named generation of an IoT Botnet Dataset in a Medium-sized IoT Network (Guerra-Manzanares et al., 2020) .Similarly, new dataset for the classification of attacks in IoT networks was proposed by Ullah et al. (2020). The dataset is named IoTID20. It contains a wide range of attacks that are meant to demonstrate IoT environment. Neto et al (2023) released a dataset named CICIoT2023 dataset. It was argued that the dataset is a real-time dataset that can be used for benchmarking studying of very large scale attacks in IoT platforms. The CIC IoT Dataset 2023 is available at https://www.unb.ca/cic/datasets/iotdataset-2023.html.

Apart from this, a IoT intrusion dataset named Aposemat IoT-23, was released by Garcia et al (2020). It is a labelled dataset with malicious and benign IoT network traffic. Also, CICIDS2017 dataset that was released by Sharafaldin et al. (2018) is another promising dataset on attack classification in IoT. The dataset and contains different kinds of attacks including some attacks in IoT networks. Another popular dataset that is popular for intrusion detection studies in IoT environment is named Bot-iot and it released was designed by Koroniotis et al. (2019) and Koroniotis et al. (2017). Another IoT dataset is named N-BaIoT Dataset. The dataset is also very promising for the detection of IoT Botnet Attacks. It is available for download at https://www.kaggle.com/code/stefanost/iot-intrusion-detection.

4. A Survey On Ml-Based Approaches For Attack Classification In IoT

Tarek et al. (2022) built a model for the detection of attacks in IoT smart applications using machine learning approach. The authors used a public dataset named AWID for the evaluation purposes. The study emphasised the promises of t-test technique used for selecting fewer attributes. The study claimed that the approach achieved an accuracy of 99% using only 8 features. The authors further claimed that the technique used performed excellently when compared with similar studies.Mohamed et al. (2020) proposed an approach termed Rules and Decision Tree-Based Intrusion Detection System for Internet-of-Things Networks. The study made use of CICIDS2017 dataset and BoT-IoT dataset. The authors mentioned that their approach had promising results in terms of accuracy, detection rate, false alarm rate and time overhead when compared to some existing schemes.

Riaz (2022) proposed a deep learning-based ensemble classification approach for the detection of malware in IoT devices. The model built is a three step approach. The data is pre-processed using scaling, normalization, and de-noising, whereas in the second step, features are selected and one hot encoding is applied followed by the ensemble classifier based on CNN and LSTM outputs for detection of malware. The study achieved an average accuracy of 99.5%.

Tasami et al. (2022) used fridge dataset to examined six ML and DL approaches to identify and categorize IoT network attacks. He came to the conclusion that Decision Tree and Random Forest performed better than 99% of the time in both binary and multiclass classification. Alzahrani and Bamhdi (2022) proposed a system to assist in the detection of botnet assaults on IoT devices. This was accomplished by creatively fusing the model of a Convolutional neural network with a long short-term memory (CNN-LSTM) algorithm. The mechanism was targeted at identifying the two frequent and dangerous IoT threats (Bashlite & Mirai 2022) on four different kinds of security cameras. The Provision PT-737E camera produced the following weighted average results for identifying the botnet: camera recall is 87%, precision is 88%, and the F1 score is 83%.The Provision PT-838 camera's classification method for botnet attacks and regular packets yielded results of 89% recall, 85% F1 score, and 94% precision. The advanced DL-based model intelligent security system proved successful in identifying botnet attacks that infected camera equipment connected to IoT applications.

Similarly, Saheed, Abiodun, Misra, Holone, and Colomo (2022) investigated the viability of deploying machine-learning-based intrusion detection in resource-constrained IoT environments, and they skilfully combined feature dimensionality reduction and machine learning methods to build an intelligent intrusion detection system (IDS) capable of detecting abnormal behaviour on insecure IoT networks. The validity dataset, accuracy, area under the curve, recall, F1, precision, kappa, and Mathew correlation coefficient (MCC) were used to analyse the experiment outcomes of his findings. His results were competitive with an accuracy of 99.9% and an MCC of 99.97% when compared to other works that had been done before.In a study on intrusion detection systems for IoT networks, In three phishing datasets, Oyelakin (2021) employed a variety of techniques for the detection of phishing evidence. In three different phishing datasets, he examined the effectiveness of the Random Forest, K-Nearest Neighbor, and Extratree algorithms. The method employed gave researchers looking at phishing detection more information. According to his findings, Random Forest outperforms the other two classifiers in terms of overall performance.

Charbuty and Abdulazeez, (2021) identified decision trees as one of the potent techniques frequently employed in a variety of disciplines, including machine learning, image processing, and pattern recognition. A succession of fundamental tests, where a numerical feature is compared to a threshold value in each test, are effectively and cogently united by the successive model known as DT.

Random forest approach was used by Maheshi (2021) to assess the feature importance score for each of the 33 features in the original dataset. Using random sampling of feature sets and the Monte Carlo method, various machine learning models were trained based on the relevance of the features. Following a thorough study of the data, the author come to the conclusion that in resource-constrained circumstances, it is sufficient to focus just on 10 characteristics, namely tcp.time_delta, "mqtt.msgid," "mqtt.hdrflags," "mqtt.msg," "tcp.len," "mqtt.len," "tcp.flags," and "mqtt.m”

By using a disagreement-based semi-supervised learning algorithm for CIDSs, Wenjuan, WeizhiMeng, and Man (2020) concentrated on semi-supervised learning and design DAS-CIDS. The authors evaluated the effectiveness of DAS-CIDS in terms of detection performance and false alarm reduction using both datasets and in actual IoT network scenarios. The experimental findings demonstrate that his technique, which automatically uses unlabelled data, is more effective in identifying intrusions and decreasing false alarms than typical supervised classifiers.

Furthermore, Kaliyar et al. (2020) in their study gave a succinct overview of two significant risks to RPL known as wormhole and sybil attacks. In Cooja, the Contiki network emulator, he applied the two methods. The outcomes of his tests show that the hypotheses about true positive rate, detection time, packet loss ratio, memory usage, and network overhead are plausible. Anwer et al. (2021) proposed a framework for the detection of malicious network traffic. The approach made use of Support Vector Machine (SVM), Gradient Boosted Decision Trees (GBDT), and Random Forest (RF) algorithms. It was reported that the model with RF learning algorithm achieved an accuracy of (85.34%). Hussain et al. (2020) built machine learning-based models for the detection of Denial of Services (DOS) and Distributed Denial of Service (DDoS) attacks in IoT networks. The authors pointed out that their proposed methodology accomplished 99.99% accuracy for the DoS and DDoS attacks in case of binary classification.

Alsamiri and Alsubhi (2019) evaluated various detection techniques using a botnet IoT dataset. Seven different machine learning algorithms were used throughout the implementation phase, and the majority of them produced excellent results. In comparison to research from the literature, new features that were retrieved from the Bot-IoT dataset during implementation produced better results. Shaikh et al. (2018) proposed a unique model that employs machine learning (ML) approaches to categorize harmful Internet of Things (IoT) traffic. The model achieved good recall and precision scores using the Gradient Boosting and Random Forest classification algorithms. Yaser and Mohammad (2012) used an artificial bee colony for attack detection based on anomalies. Additionally, it employed two feature selection methods to cut down on the volume of information needed for detection and categorization. The suggested algorithm was assessed using the KDD Cup 99 dataset. According to the findings of the experiment, an artificial bee colony can predict attacks with an average accuracy rate of 97.5% for known attacks and 93.2% for both known and unknown attacks. Fatai and Safiriyu (2012) conducted a study in which computational intelligence algorithms were shown to demonstrate their respective capabilities to produce high performance accuracy in a variety of applications. They concluded by presenting suggestions for the creative fusion and integration of individual, pre-existing techniques in new and more effective hybrid and ensemble algorithms as applied to attack detection

5. Findings and Discussion

This study sourced for relevant literature from notable repositories that focus on providing insights on datasets and works on IoT intrusion detection. Some of the recent datasets and ML-based studies for attack classification in IoT environments were surveyed . The study carried out the survey based on the chosen search strings that are deemed very relevant.. The study provided clear directions to researchers working in this area of researches. It was observed that many of the new datasets being released for intrusion detection studies contain a wide range of attacks and many of them happen in IoT networks. It was equally noticed that ML-based approaches are very popular for attack classifications in networks generally. It was equally discovered that there are different traffic features in each of the datasets. These attributes are very useful to categorising patterns of intrusions and non-intrusions in each of the dataset studied. The survey showed that most of these datasets are publicly available, which means that researchers are allowed to use them in their researches at no cost. There are equally few datasets for attack classification IoT environments that have to be paid for. Findings also revealed that some of the ML-based studies that were sourced used the following as metrics: accuracy, precision, recall, f-measure, AUC-ROC, Kappa Statistics for evaluating the performances of the learning-based attack classification models.

6. Conclusion and Future Work

This paper surveyed works that focus on intrusion detection datasets in IoT environment as well as machine learning-based approaches for the classification of attacks in IoT networks. Specifically, the study identified that IoT devices are being attacked heavily due to their prevalence and usage in different domains of the economy. Some keywords were used to source for relevant literature from notable repositories. A surveyed of this literature was done based on the two identified categories: recent datasets that are very promising for ML-based studies in attack classification in IoT environments as well as proposed ML-approaches for the classification of attacks in IoT networks. The study provided clear directions to researchers working in this area of researches by catalysing them into actions. The study started by identifying some of the growing datasets that are very popular in the cyber security domain as well a survey of some of the works that used innovative ML (Shallow and Deep Learning) approaches that classify attacks. Future work focuses on building improved ML-based detectors of attacks in IoT environment. The improvement can be achieved through a wide range of innovative approaches at any of the stages of ML workflow.

References

[1] Alatram Alaa, Sikos Leslie F.,Johnstone Mike, SzewczykPatryk, Kang James Jin (2023). DoS/DDoS-MQTT-IoT: A dataset for evaluating intrusions in IoT networks using the MQTT protocol,*Computer Networks*, 231,2023,109809,ISSN 1389-1286,

[2] Alladi, T., Chamola, V., Sikdar, B., & Choo, K. K. R. (2020). Consumer IoT: Security vulnerability case studies and solutions. *IEEE Consumer Electronics Magazine*, *9*(2), 17-25.

[3] Alsamiri, J., &Alsubhi, K. (2019). Internet of things cyber-attacks detection using machine learning. *International Journal of Advanced Computer Science and Applications*, Vol. 10, No. 12.

[4] Alzahrani, M. Y., & Bamhdi, A. M. (2022). Hybrid deep-learning model to detect botnet attacks over internet of things environments. *Soft Computing*, *26*(16), 7721-7735.

[5] Anwer M., Khan S. M., Farooq M. U., and . Waseemullah (2021). Attack Detection in IoT using Machine Learning, *Eng. Technol. Appl. Sci. Res.*, 11(3), 7273–7278, Jun. 2021.

[6] Bezerra, V.H., Costa, V.G.T., Martins, R.A., Barbon Junior, S., Miani, R.S., & Zarpelão, B.B. (2018). Providing IoT host-based datasets for intrusion detection research. *XVIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais* (SBSeg 2018)

[7] CAIDA (2007).The CAIDA DDoS Attack 2007 Dataset, available at https://www.caida.org/catalog/datasets/ddos-20070804_dataset/

[8] Charbuty, B., &Abdulazeez, A. (2021). Classification based on decision tree algorithm for machine learning. *Journal of Applied Science and Technology Trends*, *2*(01), 20-28.

[9] de Souza, C. A., Westphall, C. B., Machado, R. B., Loffi, L., Westphall, C. M., & Geronimo, G. A. (2022). Intrusion detection and prevention in fog based IoT environments: A systematic literature review. *Computer Networks*, 109154.

[10] Deogirikar, J., &Vidhate, A. (2017). Security attacks in IoT: A survey. In *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)* (pp. 32-37). IEEE.

[11] Dissanayake, M. B. (2021). Feature Engineering for Cyber-attack detection in Internet of Things. *International Journal of Wireless and Microwave Technologies*, *11*(6), 46-54.

[12] Fatai A. and Safiriyu I. E. (2012) Application of artificial intelligence in network intrusion detection. World applied programming, 158-166 ISSN: 2222-2510.

[13] Garcia Sebastian, Parmisano Agustin, & Erquiaga Maria Jose (2020). IoT-23: A labeled dataset with malicious and benign IoT network traffic (Version 1.0.0) [Data set], Zenodo. http://doi.org/10.5281/zenodo.4743746"

[14] Guerra-Manzanares, A., Medina-Galindo, J., Bahsi, H. and Nõmm, S.(2020).MedBIoT: Generation of an IoT Botnet Dataset in a Medium-sized IoT Network, DOI: 10.5220/0009187802070218, In Proceedings of the 6th International Conference on Information Systems Security and Privacy (ICISSP 2020), pages 207-218, https://www.researchgate.net/publication/338765489_MedBIoT_Generation_of_an_IoT_Botnet_Dataset_in_a_Medium-sized_IoT_Network

[15] Haji, S. H., & Ameen, S. Y. (2021). Attack and anomaly detection in iot networks using machine learning techniques: A review. *Asian journal of research in computer science*, *9*(2), 30-46.

[16] Sharafaldin Iman, Lashkari Arash Habibi, and Ghorbani Ali A. (2018). Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization, *4th International Conference on Information Systems Security and Privacy (ICISSP), Portug*al, January 2018

[17] Koroniotis, N.; Moustafa, N.; Sitnikova, E.; Turnbull, B. Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset. *Future Gener. Comput. Syst.* 2019, 100, 779–796.

[18] Koroniotis, N.; Moustafa, N.; Sitnikova, E.; Slay, J. Towards developing network forensic mechanism for botnet activities in the IoT based on machine learning techniques. *In Proceedings of the International Conference on Mobile Networks and Management, Melbourne, Australia*, 13–15 December 2017; Springer: Cham, Switzerland, 2017.

[19] Hussain Faisal, Abbas Syed Ghazanfar, Husnain Muhammad, Fayyaz Ubaid U., Shahzad Farrukh, Shah Ghalib A.(2020). IoT DoS and DDoS Attack Detection using ResNet,*Conference: 2020 IEEE 23rd International Multitopic Conference (INMIC)*, DOI: 10.1109/INMIC50486.2020.9318216

[20] Ibitoye, O., Shafiq, O., &Matrawy, A. (2019). Analyzing adversarial attacks against deep learning for intrusion detection in IoT networks. In *2019 IEEE global communications conference (GLOBECOM)* (pp. 1-6). IEEE.

[21] Ignacio P.R and Maria M R (2008) evaluation of current is intrusion detection system. *International journal LITH-ISY-EX*—08/4160---SE.

[22] Jimoh, R. G., Oyelakin, A. M., Olatinwo, I. S., Obiwusi, K. Y., Muhammad-Thani, S., Ogundele, T. S. &Ayepeku, O. F. (2022). Experimental evaluation of ensemble learning-based models for twitter spam classification. In *2022 5th Information Technology for Education and Development (ITED)* (pp. 1-8). IEEE.

[23] Kaliyar, P., Jaballah, W. B., Conti, M., & Lal, C. (2020). LiDL: localization with early detection of sybil and wormhole attacks in IoT networks. *Computers & Security*, *94*, 101849.

[24] Mohamed Amine Ferrag , Leandros Maglaras , Ahmed Ahmim , Makhlouf Derdour and Helge Janicke (2020). RDTIDS: Rules and Decision Tree-Based Intrusion Detection System for Internet-of-Things Networks, *Future Internet*, 12, 44; doi: 10.3390/fi12030044, www.mdpi.com/journal/futureinternet

[25] Neto E. C. P., Dadkhah S., Ferreira R., Zohourian A., Lu R., Ghorbani A. A. (2023). CICIoT2023: A real-time dataset and benchmark for large-scale attacks in IoT environment, Sensor (2023)

[26] Oyelakin, A. M. (2021). An Investigation into the Performances of Supervised Learning Algorithms in Different Phishing Datasets. *Pakistan Journal of Engineering, Technology & Science*, *9*(2).

[27] Oyelakin A.M. & Jimoh R.G. (2020).The Paradigm Shift of Centralised Botnets to Decentralised DGA-Botnets in the Underground Cyber Economy: An Overview, *Journal of Computer Science and Control Systems*, Faculty of Engineering and Computer Science, Oredia University, Romania 13(1), 48-51, available at https://electroinf.uoradea.ro/images/articles/CERCETARE/Reviste/JCSCS/JCSC_V13_N1_may2020/JCS CS VOL 13 NO 1 MAY 2020 Oyelakin_The_Paradigm.pdf

[28] Riaz, S.; Latif, S.; Usman, S.M.; Ullah, S.S.; Algarni, A.D.; Yasin, A.; Anwar, A.; Elmannai, H.; Hussain, S. Malware Detection in Internet of Things (IoT) Devices Using Deep Learning. *Sensors*, 2022, 22, 9305. https://doi.org/10.3390/s22239305

[29] Saheed, Y. K., Abiodun, A. I., Misra, S., Holone, M. K., & Colomo-Palacios, R. (2022). A machine learning-based intrusion detection for detecting internet of things network attacks. *Alexandria Engineering Journal*, *61*(12), 9395-9409.

[30] Shaikh, F., Bou-Harb, E., Crichigno, J., & Ghani, N. (2018). A machine learning model for classifying unsolicited IoT devices by observing network telescopes. In *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)* (pp. 938-943). IEEE.

[31] Statista, 2023. Reports on Attacks on Internet of Things Devices

[32] Tarek Gaber, Amir El-Ghamry, Aboul Ella Hassanien (2022). Injection attack detection using machine learning for smart IoT applications, *Physical Communication*, Volume 52,2022,101685,ISSN 1874-4907,https://doi.org/10.1016/j.phycom.2022.101685.

[33] Tasnim, A., Hossain, N., Parvin, N., Tabassum, S., Rahman, R., & Hossain, M. I. (2022, March). Experimental Analysis of Classification for Different Internet of Things (IoT) Network Attacks Using Machine Learning and Deep learning. In *2022 International Conference on Decision Aid Sciences and Applications (DASA)* (pp. 406-410). IEEE.

[34] Ullah I. and Mahmoud Q. H. (2020). A Scheme for Generating a Dataset for Anomalous Activity Detection in IoT Networks, In: Goutte C., Zhu X. (eds) Advances in Artificial Intelligence. Canadian AI 2020. *Lecture Notes in Computer Science*, vol 12109. Springer, Cham. https://doi.org/10.1007/978-3-030-47358-7_52