Pragmatic Study of Botnet Attack Detection In An IoT Environment

Rajasree Vennapureddy[1,a*] and T.Srinivasulu[2,b]

[1,2] Electronics & Communication Engineering, Kakatiya University, Warangal, Telangana, India

Abstract. A comprehensive search for primary research published between 2014 and 2023 was carried across several databases. Studies that describe the application of machine learning (ML) and deep learning techniques for if they was carried out across several databases. Studies that described the application of deep learning (DL) and machine learning (ML) methods for IoT botnet attack detection. Numerous facets of contemporary life have been transformed by the Internet of Things (IoT), including home automation, industrial control systems, healthcare, and transportation. On the other hand, as more devices become connected, security risks have also increased, especially from botnets. IoT Botnet attack detection techniques utilizing ML and DL have been developed in order to reduce these dangers. The best DL and ML techniques for IoT botnet attack detection are identified by a detailed examination of evaluation criteria, and performance measures in this systematic review. Performance metrics from well-known machine learning models are used to illustrate how well these machine learning techniques detect and stop Botnet attacks. When it comes to detecting Botnet assaults, deep learning (DL) and traditional machine learning (ML) methods perform similarly well. Furthermore, traditional machine learning systems still have challenges with real-time monitoring, timely detection and adaptability to novel attack approaches.

Keywords: Machine Learning (ML), Botnet attack, deep learning (DL), Internet of Things (IoT), Performance metrics, Accuracy detection, Support Vector Machine (SVM), K-Nearest Neighbor (KNN)

1. Introduction

A single botmaster controls a network of infected interconnected devices is known as a botnet. They are capable of executing a wide variety of harmful operations such as DDoS assaults, phishing schemes and spam distribution. Therefore, the every presence of networks poses a severe danger to their integrity and security (Winkler and Gomes, 2017) [1]. An item network that is connected to the internet is referred to as the Internet of Things (IoT) including medical equipment, industrial sensors, smart phones, and smart home appliances. The words "robot" and "network" are the root of the word "botnet." According

[a]rajasree.mitta@gmail.com

to (Grizzard et al. 2017)[2], a bot is a program that works autonomously and without human input to accomplish user-centric tasks. Botnet architectures can be classified into two categories: decentralized (peer-to-peer) and centralized client- server. Bots are operated differently in each of these scenarios. In a centralized client-server system, all bots are managed by a botmaster who supervises and commands them from a single, central location using command and control server. Every bot functions as a server as well as client that sends and accepts commands in a decentralized way (Beltrán-García et al. (2019)[3].To protect the security and privacy of IoT networks, Devices and end users, it is crucial to develop efficient botnet detection tools. Several connected devices are growing quickly as IoT technologies gain popularity and are used more widely, raising the possibility of cyber attacks taking advantage of these devices' weaknesses. Botnet detection usually involves machine learning techniques like SVM, random forests, Naive Bayes, decision trees and KNN. (Nazir & Associates, 2023)[4] The efficacy of these techniques is significantly influenced by the caliber of the datasets utilized for training and evaluation. These datasets contain labeled information about network traffic, covering both good and bad actions. Analyzing the subject in-depth will highlight the gaps and difficulties that need to be addressed in future research to improve the security of IoT devices, as well as help determine which ML and DL algorithms are most effective at identifying IoT botnet attacks. (Williams et al. 2022)[5]The literature now has a large number of survey studies that discuss the details of applying machine learning techniques for IoT botnet identification.

1.1 Objectives: The need for effective detection techniques and the growing awareness of the threats posed by Internet of Things botnets are what motivated this review paper. The weaknesses and possibilities for widespread botnet attacks associated with the Internet of Things are becoming more and more evident as it grows. Methods such as ML and DL have demonstrated great potential in resolving this problem. However, a comprehensive study and analysis of the body of recent literature is required in order to properly comprehend state-of-the-art methodologies, their efficacy, limits, and possibilities for future research. By providing practitioners, academics and policymakers with a comprehensive overview of ML or DL based IoT botnet detection, we hope to increase awareness of the subject and guide the implementation of trustworthy and efficient detection methods.

The research topics that guided our systematic review of ML/DL-based IoT botnet detection are presented in this part. These study subjects provided a structure and boundaries for our evaluation, allowing us to explore important fields including deep learning and machine learning methods, reference datasets, and performance measures related to IoT botnet detection.

- What motivations drive the creation of botnet attacks?
- How have assaults using botnets changed over time?
- What solutions has the scientific community offered to lessen the harm posed by botnets?
- What are the current botnet trends and issues that modern research has identified?

1.2 Botnet Detection Types and Techniques:

Some of the types and techniques of botnet detection were explained below. Decision trees are the most advanced and efficient method for categorization and forecasting. An example of a tree structure that looks like a flowchart is called a decision tree. A decision tree has an inner node for each attribute, a branch for the test result, and a class label for each leaf node, or terminal node. Decision trees are flexible machine learning models that may be

used not only for IoT botnet detection but also for regression and classification issues, in addition to IoT botnet Detection. The Naive Bayes Classifier is a collection of Bayes based classification method. Rather than being a single algorithm with shared notions, this is a family of algorithms. Each categorized pair of features is distinct from the others. The basic assumption of the naïve Bayes classifier (NBC) is that the characteristics are independent of the class. One of the most significant and fundamental machine learning classification techniques is K-Nearest Neighbors. It is frequently used in pattern recognition, data mining, and intrusion detection and falls under the domain of supervised learning. For regression and classification problems, K- nearest neighbor is a popular machine learning technique (Xiong & Yao, 2021)[6]. The similarity principle, which states that cases are grouped according to how closely their features resemble those of known instances, is the foundation of this algorithm. In KNN, a given instance is categorized or assigned a value according to its k closest neighbors. The efficiency of the method may be impacted by the k value, which is frequently selected empirically. Using network traffic data, KNN is used for classifying tasks to locate IoT botnets (Isnain et al., 2021)[7]. By gathering characteristics from network traffic like count, byte distribution and packet length. KNN may classify data as safe or infected to botnet. A number of variables, such as feature selection, k value, and dataset size, affect how well KNN detects botnets (Kumar and Lim, 2019).[8]. The Support vector machines which is a supervised machine learning techniques is used for regression and classification (Leevy et al., 2022).[9]. The main objective of the SVM technique is to find the best hyper plane for successfully differentiating between different classes of data by maximizing the margin between the support vectors or the nearest points from each class. SVM is widely used in speech recognition, picture classification, anomaly detection, and other domains. Interestingly, it has also been used to locate Internet of Things botnets, which pose a significant risk to network security (Atzori et al., 2010)[10].

2. Discussion

2.1 Architecture of IoT: The IoT is a rapidly expanding field of technology with many applications. The design and growth of the IoT determines how it works and is dependent on its several application sectors. Nevertheless, it does not have a specified architecture of operation that is universally followed (Abed et al. 2016)[11]. The architecture of IoT is determined by how it functions and is used in different sectors. Smart gadgets, not the world's population, are the primary driver of this growth (Alam et al., 2018)[12]. Integrated technologies are essential for linking physical objects and facilitating information transmission between them (Aljohani et al., 2015). [13]

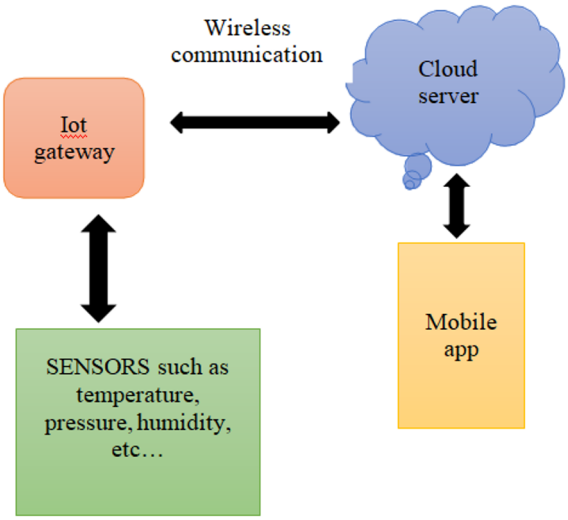

Figure1: IoT Architecture

This setting allows both humans and machines to communicate with one another (machine-to-machinecommunication). The combination of embedded items, smartdevices, and the IoT with smart buildings, smart cars, and network connections to share information amongst physical items, smart devices, sensors, actuators, and programs. The wireless sensor network had a major role in the development of the IoT idea.

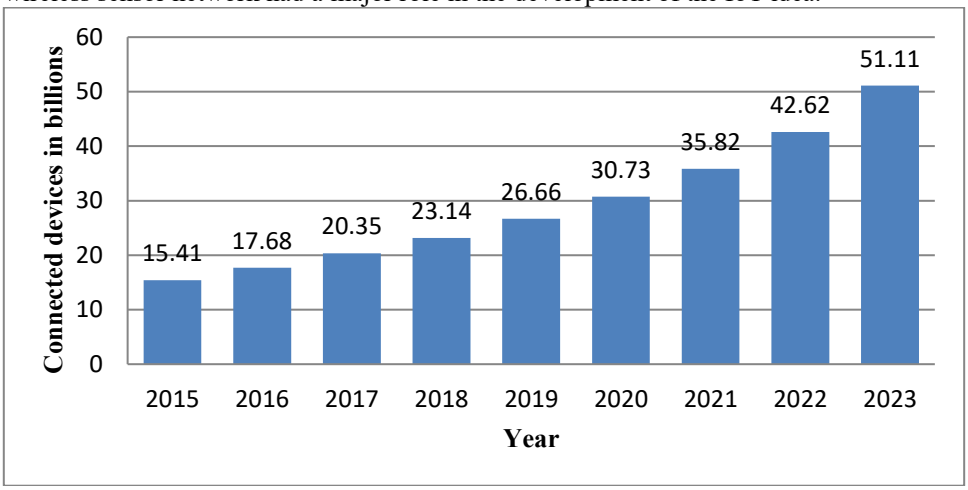

Figure 2: IoT connected devices

2.2 AI based Machine Learning: The IoT sector has made great strides toward achieving sustainable development goals thanks to the application of AI-ML technologies. AI-driven ML revolutionary potential has ushered in a new era in healthcare by upending established procedures and inspiring a paradigm shift toward more innovative, efficient, and equitable healthcare services. (Bajwa et al. 2021)[17]. In light of concerns about global health and the need for sustainable healthcare systems. This study explores the potential significant effects of AI-enabled machine learning systems on improving delivery of healthcare services.

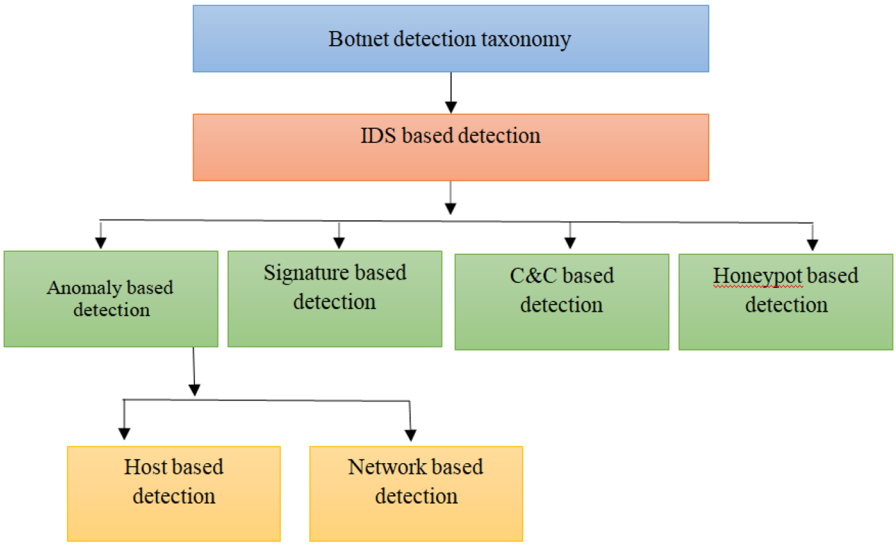

Figure 3: Botnet detection taxonomy

Cutting edge technology, healthcare and data analytics have joined forces to solve significant issues in disease detection, accessibility to healthcare services, treatment efficacy, resource allocation, and clinical workflow optimization (Kasula et al., 2023)[18]. In 2020, Soe et al. [25] developed a sequential detection architecture botnet assault detection system that is based on machine learning. The implementation of a high-performing, lightweight detection system makes use of an effective feature selection strategy.

Using three separate machine learning algorithms the artificial neural network, J48 decision tree and Naive Bayes method. Botnet attack detection achieves over 99% overall detection performance. Using an efficient deep neural network (DNN) architecture, network traffic is classified (Popoola et al., 2021).[26]. The independent DNN model training in various IoT edge devices is remotely coordinated by a model parameter server, and the local model updates are aggregated using the federated averaging (FedAvg) technique. Several rounds of communicationbetween the model parameter server and the IoT-edge devices,a global DNN model is built. Using the N-BaIoTand Bot-IoT data sets are used to mimic zero-day botnet attack scenarios in IoT edge devices (Allison and others, 2022) [27]. The majority ofmachine learning-based methods for detecting botnets are restricted to a certain dataset. The variability of attack patternscauses these approaches to perform badly on various datasets. use ensemble learning to profile behavior aspects of IoT networks and detect aberrant network traffic from hacked IoTdevices.

In the future, a big data collection will be able to be usedto train the model. It is also possible to test machine learningclassifiers like Random Forest and SVM. Deep learning models can be utilized for botnet identification in addition to ResNet50 and LSTM models. The ELBA-IoT ensemble learning model is developed in (Abu Al-Haija et al. (2022))[28], used ensemble learning to profile behavior aspects of IoT networks and detect network traffic from hacked IoT devices.

Table 1: The Evaluation Of Recent Research DoneIn The Field of IoT Security

Study	**DL Based**	**ML Based**	**IoT Botnet model**

Miller et al.(2016)[19]	**x**	□	□□
Koroniotis et al. (2018)[20]	**x**	□	□□
Salim et al.(2019)[21]	□□□	**x**	**x**
Soe et al.(2020)[22]	**x**	□	□□
Alharbi et al.(2021)[23]	**x**	**x**	□□
Rbah et al. (2023)[24]	□□□	**x**	□□

Using an IoT based Botnet detection strategy, three distinct ML techniques—AdaBoosted, RUS Boosted, and bagged—that are a part of decision tree methodology are evaluated. ELBA-IoT was evaluated using data from the N-BaIoT-2021 dataset, which captures both normal IoT network traffic and Botnet attack traffic of compromised IoT devices. The experimental results show that our suggested ELBA-IoT has high detection accuracy (99.6%) for Botnet attacks coming from compromised IoT devices.

Long-term correlated changes can be seen in low dimensional feature set generated by LAE using deep bidirectional long short term memory (BLSTM) (Popoola et al. 2020)[29]. BoT-IoT data collection is used in many trials to test the efficacy of the proposed hybrid deep learning technique. Outcomes demonstrated that the memory space needed to store large-scale network traffic data was greatly decreased by 91.89%, and that LAE outperformed state-of-the-art feature dimensionality reduction approaches by 18.92–27.03%. Alkahtani et al. (2021) [30]. An detailed empirical investigation was carried out with an N-BaIoT dataset from the real world that contained both benign and dangerous patterns. The testing results revealed that the CNN-LSTM model is superior in identifying botnet attacks, with accuracies of 90.88% and 88.61%. Nevertheless, the recommended technique had a good accuracy of 88.53%.

3. Review of Literature

The internet of things is being used in more and more ways every day. As a result, worries about information security are growing. In the suggested system (Lin et al. 2014)[31], support vector machines and artificial fish swarm algorithms are combined. Using connection logs, Mahardhika et al. (2017)[32] explain how the network flow approaches the dataset. The rule induction algorithm achieves up to 98% accuracy. This article (Niranjan et al. 2018)[33] proposes merging KNN, the Naïve Bayes kernel, and the ID3 classifier to develop a model that yields more accurate results. EKNIS is essentially a hybrid approach that blends the Naïve Bayes Kernel, k Nearest Neighbor (KNN), and ID3.

Table 2: Comparison Table

Reference	**Methods**	**Accuracy Rate**
Lin et al. (2014)	Artificial fish swarm algorithm	97.7%

Mahardhika et al. (2017)	Rule induction algorithm, K- nearest neighbor, decision tree, naive bayes	98.8%
Niranjan et al. (2018)	KNN, Naïve Bayes Kernel and ID3	99.8%
Savenko et al. (2019)	Naive Bayes	88.0%
Bijalwan et al. (2020)	Ensemble of KNN and decision tree algorithm	96.4%
Shareena et al. (2021)	Naive- Bayes, SVM, decision tree, random forest	93.0%
Raghavendra et al. (2022)	IPR algorithm and decision tree	99.0%
Schmitt et al. (2023)	Logistic regression, random forest, gradient boosting	98.0%

There have been two datasets used: scenario-2 and scenario-6. There are two levels to the Botnet detection technique covered in this paper (Savenko et al., 2019)[34]: host and network. It finds bots at the host level using a Bayes classifier, and it determines the likelihood that a botnet is present in the network by utilizing the entire distributed system. This created classifier demonstrates an accuracy of roughly 88%. To assess Botnet traffic, this research (Bijalwan et al. 2020)[35] uses an ensemble of classifier algorithms. For IoT networks, we build a highly adaptable Deep Neural Network (DNN) that can recognize threats from IoT bonnets. Altogether Shareena (2021)[36] According to the investigation, our DNN operates remarkably gracefully and precisely better than the other systems. The results show that using an ensemble of classifiers works better than using a single classifier when it comes to uncovering bot evidence. Accuracy is improved by soft voting using KNN and Decision Tree. The approach proposed by Raghavendra et al. (2022)[37] utilizes datasets containing Mirai and Bashlite. The nine most important features that let IoT devices to separate between normal traffic and abnormal traffic are identified using the XGBoost IPR algorithm. Nonetheless, the decision tree is recommended since it is simpler and more accurate. (2018) Meidan et al. [38]. The recently developed N-BaIoT, a network-based anomaly detection method for the Internet of Things, detects unusual network traffic from infected IoT devices by using deep autoencoders and network behavior snapshots. There are several methods for identifying botnets. (Hussain et al. 2020)[39], however how good they are depends on the dataset they are trained on. This is a result of the attack behaviors unpredictability; features that were employed to train a ML model on one Botnet dataset do not translate well to other datasets.

(Waqas et al. 2022)[40] The most crucial concerns are security-related, and many models have been developed to solve these problems. Nevertheless, new botnet attack variants, including Mirai, Persirai, and Bashlite, continue to emerge and take advantage of security flaws. (Popoola et al.2021)[41] For deep learning (DL) on an IoT back-end server, storing and transferring data will require a big memory space and high network bandwidth for high feature dimensionality in the training data. The DRNN approach produces low performance in minority classes when data has very unequal network traffic. In 2020, the Alqahtani group [42] The Bot-IoT dataset is used to evaluate this method's efficacy. The findings demonstrated that reducing the dimension of the network traffic features in the training set using the LAE approach resulted in an 86.49% reduction in the amount of memory needed

for data storage. In order to protect today's digital ecosystems, this study (Schmitt et al. 2023)[43] examines the use of artificial intelligence in cyber threat identification. In the areas of mobile security, network security and Internet of Things security, the main emphasis is on assessing ML based classifiers and groups for anomaly-based malware detection and detection of network intrusions, as well as how to combine those models. Khazane et al. (2024) [44] In addition to offering answers, the session discusses the challenges issues of integrating AI enabled cyber security solutions for current IT infrastructures and business processes.

A total accuracy rate of 98% was achieved by gathering three sets of data, identifying them using deep learning. (Sharma et al.2023)[45]Because botnets are evolving to incorporate structural changes and the use of obfuscation techniques on packet data, researchers working on detection models are facing challenges. In 2023, Meziane et al.[46]-A multitude of studies show that traditional signature-based or content-based methods are ineffective in identifying botnets. Nevertheless, behavior-based and IOT-based approaches may be used to overcome the problem (Woodiss-Field et al. 2024)[47]. As demonstrated by the comparison with earlier research on the topic, researchers usually only develop botnet detection for a certain structure and protocol. In 2021, Pokhrel et al.[48] IoT security is regarded as one of the major challenges. The primary goal of this study is to create a novel model that detects and stops distributed denial of service assaults in botnet-powered IoT networks using a ML algorithm. (Singh et al. 2023)[49] IoT network-connected sensors and actuators are low-power and have limited memory. IoT devices are inherently vulnerable, meaning that an attacker can always hack them and exploit them to create a sizable botnet. An extensive analysis of IoT botnet attacks is provided, including with statistics and botnet architectures. (Sharma et al. 2023)[50] It's critical to take into account any security vulnerabilities that could enable effective IoT assaults.

Conclusion

In this work, parameter of accuracy for a botnet detection system are discussed and data from multiple research publications are presented and analyzed. Given that several techniques are currently in place to identify bots within a system or data source. Learn about the many algorithms that are employed to find botnets in datasets. This document provides an overview of the many algorithms that are utilized as well as their outcomes. Depending on the algorithm employed for the dataset in a given system, the accuracy parameter yields varying outcomes. The parameter varies depending on the system.

References

[1] Winkler, Ira, and Araceli Treu Gomes. Advanced persistent security: a cyberwarfare approach to implementing adaptive enterprise protection, detection, and reaction strategies. Syngress, 2016.

[2] Grizzard, J.B.; Sharma, V.; Nunnery, C.; Kang, B.B.; Dagon, D. Peer-to-Peer Botnets: Overview and Case Study. In *First Workshop on Hot Topics in Understanding Botnets (HotBots 07)*; USENIX Association: Cambridge, MA, USA, 2007.

[3] Beltrán-García, P.; Aguirre-Anaya, E.; Escamilla- Ambrosio, P.J.; Acosta-Bermejo, R. IoT Botnets. In *Communications in Computer and Information Science*; Springer International Publishing: Merida, Mexico, 2019; pp. 247–257

[4] Nazir, Ahsan, Jingsha He, Nafei Zhu, Ahsan Wajahat, Xiangjun Ma, Faheem Ullah, Sirajuddin Qureshi, and Muhammad Salman Pathan. "Advancing IoT security: A systematic review of machine learning approaches for the detection of IoT botnets."

Journal of King Saud University-Computer and Information Sciences (2023): 101820.

[5] Williams, Phillip, Indira Kaylan Dutta, Hisham Daoud, and Magdy Bayoumi. "A survey on security in internet of things with a focus on the impact of emerging technologies." *Internet of Things* 19 (2022): 100564.

[6] Xiong, Lei, and Ye Yao. "Study on an adaptive thermal comfort model with K-nearest-neighbors (KNN) algorithm." *Building and Environment* 202 (2021): 108026.

[7] Isnain, Auliya Rahman, Jepi Supriyanto, and Muhammad Pajar Kharisma. "Implementation of K- Nearest Neighbor (K-NN) Algorithm For Public Sentiment Analysis of Online Learning." *IJCCS (Indonesian Journal of Computing and Cybernetics Systems)* 15, no. 2 (2021): 121-130.

[8] Kumar, Ayush, and Teng Joon Lim. "Early detection of Mirai-like IoT bots in large-scale networks through sub- sampled packet traffic analysis." In *Advances in Information and Communication: Proceedings of the 2019 Future of Information and Communication Conference (FICC), Volume 2*, pp. 847-867. Springer International Publishing, 2020.

[9] Leevy, Joffrey L., Taghi M. Khoshgoftaar, and John Hancock. "Feature evaluation for IoT botnet traffic classification." *International Journal of Internet of Things and Cyber-Assurance* 2, no. 1 (2022): 87-102.

[10] Atzori, Luigi, Antonio Iera, and Giacomo Morabito."The internet of things: A survey." *Computer networks* 54, no. 15 (2010): 2787-2805.

[11] Abed, Ali Ahmed. "Internet of Things (IoT): architecture and design." In 2016 Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications (AIC-MITCSA), pp. 1-3. IEEE, 2016.

[12] Alam, Tanweer. "A reliable communication framework and its use in internet of things (IoT)." *CSEIT1835111| Received* 10 (2018): 450-456.

[13] Aljohani, Mohammed, and Tanweer Alam. "Real time face detection in ad hoc network of android smart devices." In *International Conference on Computational Intelligence*, pp. 245-255. Singapore: Springer Nature Singapore, 2015.

[14] Alam, Tanweer. "Fuzzy control based mobility framework for evaluating mobility models in MANET of smart devices." *ARPN Journal of Engineering and Applied Sciences* (2017).

[15] Singh, Parbhakar, Parveen Kumar, and Tanweer Alam. "Generating different mobility scenarios in ad hoc networks." *International Journal of Electronics Communication and Computer Technology* 4, no. 2 (2014): 582-591.

[16] Zhang, Hongfei, Li Zhu, Tao Dai, Liwen Zhang, Xi Feng, Li Zhang, and Kaiqi Zhang. "Smart object recommendation based on topic learning and joint features in the social internet of things." *Digital Communications and Networks* 9, no. 1 (2023): 22-32.

[17] Bajwa, Junaid, Usman Munir, Aditya Nori, and Bryan Williams. "Artificial intelligence in healthcare: transforming the practice of medicine." *Future healthcare journal* 8, no. 2 (2021): e188.

[18] Kasula, Balaram Yadav, and Pawan Whig. "AI-Driven Machine Learning Solutions for Sustainable Development in Healthcare—Pioneering Efficient, Equitable, and Innovative Health Service." *International Journal of Sustainable Development Through AI, ML and IoT* 2, no. 2 (2023): 1-7.

[19] Miller, Sean, and Curtis Busby-Earle. "The role of machine learning in botnet detection." In *2016 11th international conference for internet technology and secured transactions (icitst)*, pp. 359-364. IEEE, 2016.

[20] Koroniotis, Nickolaos, Nour Moustafa, Elena Sitnikova, and Jill Slay. "Towards developing network forensic mechanism for botnet activities in the IoT based on machine learning techniques." In *Mobile Networks and Management: 9th International Conference, MONAMI 2017, Melbourne, Australia, December 13-15, 2017, Proceedings 9*, pp. 30-44. Springer International Publishing, 2018.

[21] Salim, Mikail Mohammed, and Jong Hyuk Park. "Deep Learning based IoT re-

authentication for botnet detection and prevention." In *Advanced Multimedia and Ubiquitous Engineering: MUE/FutureTech 2019 13*, pp. 239-242. Springer Singapore, 2020.

[22] Soe, Yan Naung, Yaokai Feng, Paulus Insap Santosa, Rudy Hartanto, and Kouichi Sakurai. "Machine learning- based IoT-botnet attack detection with sequential architecture." *Sensors* 20, no. 16 (2020): 4372.

[23] Alharbi, Afnan, and Khalid Alsubhi. "Botnet detection approach using graph-based machine learning." *IEEEAccess* 9 (2021): 99166-99180.

[24] Rbah, Yahya, Mohammed Mahfoudi, Younes Balboul, Kaouthar Chetioui, Mohammed Fattah, Said Mazer, Moulhime Elbekkali, and Benaissa Bernoussi. "A machine learning based intrusions detection for IoT botnet attacks." In *AIP Conference Proceedings*, vol.2814, no. 1. AIP Publishing, 2023.

[25] Soe, Yan Naung, Yaokai Feng, Paulus Insap Santosa, Rudy Hartanto, and Kouichi Sakurai. "Machine learning- based IoT-botnet attack detection with sequential architecture." *Sensors* 20, no. 16 (2020): 4372.

[26] Popoola, Segun I., Ruth Ande, Bamidele Adebisi, Guan Gui, Mohammad Hammoudeh, and Olamide Jogunola. "Federated deep learning for zero-day botnet attack detection in IoT-edge devices." *IEEE Internet of Things Journal* 9, no. 5 (2021): 3930-3944.

[27] Alissa, Khalid, Tahir Alyas, Kashif Zafar, Qaiser Abbas, Nadia Tabassum, and Shadman Sakib. "Botnet attack detection in iot using machine learning." *ComputationalIntelligence and Neuroscience* 2022 (2022).

[28] Abu Al-Haija, Qasem, and Mu'awya Al-Dala'ien. "ELBA-IoT: an ensemble learning model for botnet attack detection in IoT networks." *Journal of Sensor and Actuator Networks* 11, no. 1 (2022): 18.

[29] Popoola, Segun I., Bamidele Adebisi, Mohammad Hammoudeh, Guan Gui, and Haris Gacanin. "Hybrid deep learning for botnet attack detection in the internet- of-things networks." *IEEE Internet of Things Journal* 8,no. 6 (2020): 4944-4956.

[30] Alkahtani, Hasan, and Theyazn HH Aldhyani. "Botnet attack detection by using CNN-LSTM model for Internetof Things applications." *Security and Communication Networks* 2021 (2021): 1-23.

[31] Lin, Kuan-Cheng, Sih-Yang Chen, and Jason C. Hung. "Botnet detection using support vector machines with artificial fish swarm algorithm." *Journal of Applied Mathematics* 2014 (2014).

[32] Mahardhika, Yesta Medya, Amang Sudarsono, and Ali Ridho Barakbah. "An implementation of Botnet dataset to predict accuracy based on network flow model." In *2017 International Electronics Symposium on Knowledge Creation and Intelligent Computing (IES- KCIC)*, pp. 33-39. IEEE, 2017.

[33] Niranjan, A., K. M. Akshobhya, P. Deepa Shenoy, and K. R. Venugopal. "EKNIS: Ensemble of KNN, Naïve Bayes Kernel and ID3 for Efficient Botnet Classification Using Stacking." In *2018 International Conference on Data Science and Engineering (ICDSE)*, pp. 1-6. IEEE, 2018.

[34] Savenko, Oleg, Anatoliy Sachenko, Sergii Lysenko, and George Markowsky. "Botnet Detection Approach for the Distributed Systems." In *2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, vol. 1, pp. 406-411. IEEE, 2019.

[35] Bijalwan, Anchit. "Botnet forensic analysis using machine learning." *Security and CommunicationNetworks* 2020 (2020): 1-9.

[36] Shareena, Jishma, Aiswarya Ramdas, and Haripriya AP. "Intrusion detection system for iot botnet attacks using deep learning." *SN Computer Science* 2, no. 3 (2021): 1-8.

[37] Raghavendra, Meghana, and Zesheng Chen. "Detecting IoT Botnets on IoT Edge Devices." In *2022 IEEE International Conference on Communications Workshops (ICC Workshops)*, pp. 373-378. IEEE, 2022.

[38] Meidan, Yair, Michael Bohadana, Yael Mathov, Yisroel Mirsky, Asaf Shabtai, Dominik Breitenbacher, and Yuval Elovici. "N-baiot—network-based detection of iot botnet attacks using deep autoencoders." *IEEE Pervasive Computing* 17, no. 3

(2018): 12-22.

[39] Hussain, Faisal, Syed Ghazanfar Abbas, Ubaid U. Fayyaz, Ghalib A. Shah, Abdullah Toqeer, and Ahmad Ali. "Towards a universal features set for IoT botnet attacks detection." In *2020 IEEE 23rd International Multitopic Conference (INMIC)*, pp. 1-6. IEEE, 2020.

[40] Waqas, Muhammad, Kamlesh Kumar, Asif Ali Laghari, Umair Saeed, Muhammad Malook Rind, Aftab Ahmed Shaikh, Fahad Hussain, Athaul Rai, and Abdul Qayoom Qazi. "Botnet attack detection in Internet of Things devices over cloud environment via machine learning." *Concurrency and Computation: Practice andExperience* 34, no. 4 (2022): e6662.

[41] Popoola, Segun I., Bamidele Adebisi, Ruth Ande, Mohammad Hammoudeh, and Aderemi A. Atayero. "Memory-efficient deep learning for botnet attackdetection in IoT networks." *Electronics* 10, no. 9 (2021):1104.

[42] Alqahtani, Mnahi, Hassan Mathkour, and Mohamed Maher Ben Ismail. "IoT botnet attack detection based on optimized extreme gradient boosting and feature selection." *Sensors* 20, no. 21 (2020): 6336.

[43] Schmitt, Marc. "Securing the Digital World: Protecting smart infrastructures and digital industries with Artificial Intelligence (AI)-enabled malware and intrusion detection." *Journal of Industrial InformationIntegration* 36 (2023): 100520.

[44] Khazane, Hassan, Mohammed Ridouani, Fatima Salahdine, and Naima Kaabouch. "A Holistic Review of Machine Learning Adversarial Attacks in IoT Networks." *Future Internet* 16, no. 1 (2024): 32.

[45] Sharma, Bhisham, Deepika Koundal, Rabie A.Ramadan, and Juan M. Corchado. "Emerging Sensor Communication Network-Based AI/ML Driven Intelligent IoT." *Sensors* 23, no. 18 (2023): 7814.

[46] Meziane, Hind, and Noura Ouerdi. "A survey on performance evaluation of artificial intelligence algorithms for improving IoT security systems." *Scientific Reports* 13, no. 1 (2023): 21255.

[47] Woodiss-Field, Ashley, Michael N. Johnstone, and Paul Haskell-Dowland. "Examination of Traditional Botnet Detection on IoT-Based Bots." *Sensors* 24, no. 3 (2024):1027.

[48] Pokhrel, Satish, Robert Abbas, and Bhulok Aryal. "IoT security: botnet detection in IoT using machine learning." *arXiv preprint arXiv:2104.02231* (2021).

[49] Singh, N. Joychandra, Nazrul Hoque, Kh Robindro Singh, and Dhruba K. Bhattacharyya. "Botnet-based IoT network traffic analysis using deep learning." *Security and Privacy* (2023): e355.

[50] Sharma, Antariksh, Vibhakar Mansotra, and Kuljeet Singh. "Detection of Mirai Botnet Attacks on IoT devices Using Deep Learning." *Journal of Scientific Research and Technology* (2023): 174-187