BOTNET DETECTION USING VARIOUS MACHINE LEARNING ALGORITHMS: A REVIEW

M.M. Swami [2], Abhilash Yadnik [1], Atharva Jagtap [1], Kshitij Bhilare [1], Mahant Wagh [1]

[2]M.M. Swami, [1]Abhilash Yadnik, [1]Atharva Jagtap, [1]Kshitij Bhilare, [1]Mahant Wagh
[1]Department of Computer Engineering, AISSMS College of Engineering, Pune, India
[2]Assistant Professor, Department of Computer Engineering, AISSMS College of Engineering, Pune, India

---***---

Abstract - *In past decades, use of internet is growing in every part of technology and which is hindered by various security issues. Relatively, it questions on data confidentiality, data integrity and data availability. One of the source of data breach is botnet and it is a threat to internet security. Therefore, to make the system robust, reliable and secure there are some mechanisms for botnet detection and removal process. Botnets are generally categorized according to the protocol used by the command-and-control server in IRC, HTTP, DNS or Peer to Peer (P2P) botnets. Botnets can be detected using various algorithms such as decision tree, random forest, KNN, K-nearest neighbor, naïve bayes, support vector machine, etc. In this paper, The analysis of various papers on botnet attacks and detection techniques.*

Key Words: **Botnet, Detection, Machine learning, Algorithms, Decision tree, Accuracy, Precision, F score, Recall.**

1. INTRODUCTION

The use of internet is growing rapidly which in turn, has brought about many cyberattacks. This cyberattacks mainly done by botnet. The increase in use of internet increases risk of attack of botnet. Botnet accounts for 80% of internet attacks in today's world. Botnet are the network of Bots which is controlled by some third-party user to carry out malicious activities. A botnet consists of three components such as botmaster, a command and control (C&C) server, and a bot. Bot performs series of malicious activities on compromised host. C&C server carried out the attacks. The differentiation between client-server model and peer-to-peer(P2P) model based on the botnet architecture or construction is done. When a user visits an infected site, the bot could be installed on their devices easily. Botnet can be used for DDOS attack, steal data, phishing, send spam, unwanted ads, generating virtual clicks and allow attacker to access our device. The increasing number of malicious attacks is a serious problem. If there is data breach, it could cost billions of dollars in damages and recovery. It has negative impact on organization reputation. To avoid such losses, The detection of botnet from the systems by using various algorithms and techniques is carried out.

2. Algorithms

Decision tree--Decision trees are the most powerful and popular classification and prediction tools. A decision tree is a flowchart-like tree structure where each inner node specifies a test for an attribute, each branch represents the result of the test, and each leaf node (terminal node) contains a class label.

Naive Bayes Classifiers-- Naive Bayes Classifier is a collection of classification algorithms based on Bayes' theorem. This is not a single algorithm, but a family of algorithms, all sharing common principles. Each pair of classified features is independent of each other.

K- Nearest Neighbor--K-Nearest Neighbors is one of the most basic and important classification algorithms in machine learning. It belongs to the field of supervised learning and is widely used in pattern recognition, data mining and intrusion detection.

Support Vector Machine-- Support vector machines (SVMs) are supervised machine learning algorithms used for both classification and regression. Also known as a regression problem, it is best suited for classification. The goal of the SVM algorithm is to find a hyperplane in the N-dimensional space that uniquely classifies the data points.

JRIP-- JRip (RIPPER) is one of the basic and most popular algorithms. Classes are examined as they grow in size and an initial rule set for the class is generated using a decreasing error. JRip treats every instance of a particular decision in the training data as a class and finds a set of rules covering all members of that class

PART-- PART is a tutorial on separate and conquer rules. This algorithm creates a rule set called a "decision list" which is a planned set of rules. New data is compared to each rule in the list in turn, and the item is assigned the class of the first matching rule. At each iteration, PART builds a partial C4.5 decision tree and transforms the "best" leaves into rules.

Clonal selection Algorithm-- A clonal selection algorithm demonstrates how the immune system responds to Ag and its enhanced ability to eliminate Ag. When Ag attacks the body, immune cells (B lymphocytes) produce -specific Abs that attack Ag. Ab's are primarily molecules that binds to the surface of B cells, whose goal is to recognize Ag's, to which binds. Given the detection characteristics of CLONALG, it could be the basis for tools in the botnet detection process.

Random Forest-- Random Forest is a popular machine learning algorithm related to supervised learning techniques. It can be used for both ML classification and regression problems. It is based on the concept of ensemble learning, which combines multiple classifiers to solve complex problems and improve model performance*.* each iteration and makes the "best" leaf into a rule

Artificial neural network-- The term "artificial neural network" describes a biologically-inspired sub-area of artificial intelligence modeled after the brain. Artificial neural networks are computer networks usually based on biological neural networks that build the structure of the human brain. Just like the human brain has neurons connected to each other, artificial neural networks have neurons connected to each other at different layers of the network. These neurons are called nodes.

Local Outlier Factor (LOF)-- The Local Outlier Factor (LOF) algorithm is an unsupervised anomaly detection method that computes local density deviations for the neighborhood of a given data point. A sample is considered an outlier with a much lower density than its neighboring samples.

Hidden Markov Model (HMM)-- A hidden Markov model (HMM) is a statistical model that can be used to describe the evolution of observable events that depend on internal factors, which are not directly observable. Call for the observed event a `symbol' and the invisible factor underlying the observation a `state'.

Artificial Fish-Swarm Algorithm (AFSA)-- AFSA (Artificial Fish-Swarm Algorithm) is one of the best optimization techniques among swarm intelligence algorithms. The algorithm is inspired by the movement of fish schools and their various social behaviors. Based on a series of instinctive behaviors, fish always try to maintain the colony and display intelligent behavior accordingly. Foraging, migrating, and dealing with danger are done in a social way, and interactions between all fish in a group result in intelligent social behavior.

3. Literature review

A brief study on Botnet Detection papers published earlier has been done and formatted in a tabular format. The addition of attributes like paper title, author name, algorithm used, and parameters.

The application of internet of things are increasing day by day. Therefore, information security concerns are increasing. In the proposed system [1], combining artificial fish swarm algorithm and support vector machine.

In the proposed system [2] usage of behavior-based botnet detection system based on fuzzy pattern recognition technique. It achieves high detection rate up to 95 %.

In this document [3], the network flow with the connection logs approaching the dataset. Rule induction algorithm gives higher accuracy up to 98%. Using ISCX dataset for research purpose. System detects botnet using these four machine learning models: Naïve bayes, decision tree, support

It [4] uses UNSW-NB15 dataset, Decision trees model gives higher accuracy than other. Various communication protocols are used by botmasters to communicate with the command-and-control server in a botnet.

The proposed system [5] detects botnets based on DNS traffic analysis. A novel hybrid rule detection model technique is proposed by the union of the output of two algorithms.

This paper [6] proposes to make a model using hybrid approach by combining KNN, Naïve bayes kernel and ID3 classifier which gives us more accurate results. EKNIS is basically a hybrid technique that involves a combination of k Nearest Neighbor (KNN), Naïve Bayes Kernel and ID3.It has used two datasets scenario-6 and scenario-2

This paper [7] gives the botnet detection technique which involves two levels: Host and Network. In host level it detects Bot using bayes classifier and in network level it estimates the probability of the botnets presence in the network using the entire distributed system. this developed classifier shows that the accuracy of this is about 88% Proposed [8] approach use the clonal selection algorithm which mainly focus on improving Bot GRABBER system. It is able to detect the IRC, HTTP, DNS and P2Pbotnets. It has high accuracy of about 95% and very low rate of false positive at about 3-5% vector.

[9] P2P botnet used multiple main controllers to avoid single point of failure, and failed various misuse detecting technologies together with encryption technologies. The data mining scheme discovers the host of p2p botnet in real internet.

This paper [10] uses the ensemble of classifier algorithm to analyses the botnet traffic. It uses ISCX dataset. results show that the performance for finding bot evidence using ensemble of classifiers is better than single classifier. Soft Voting of KNN & Decision Tree gives higher accuracy.

Proposed [11] approach uses dataset having Mirai and Bashlite. IPR algorithm with XGBoost to identify nine most

Table -1:

Paper title	**Author**	**Algorithm used**	**Parameters**
Botnet Detection Using Support Vector Machines with Artificial Fish Swarm Algorithm[1]	Kuan-Cheng Lin, Sih-Yang Chen,and Jason C. Hung	Artificial fish swarm algorithm	Accuracy rate AFSA-SVM: 97.76 GASVM: 97.30
A fuzzy pattern based filtering algorithm for botnet detection[2]	K Wang, CY Huang, SJ Lin, YD Lin	FPRF algorithm	Detection rate: 95.29 True positive rate: 95 False positive rate: 03.08
An implementation of Botnet dataset to predict accuracy based on network flow model. [3}	Mahardhika, Y. M., Sudarsono, A., & Barakbah, A. R.	Rule induction algorithm, K- nearest neighbor, decision tree, naïve bayes	Precision: 98.70 FMeasure: 99.40 Recall: 98.80 Accuracy: 98.80
Botnet Attack Detection using Machine Learning [4]	Mustafa Alshamkhany, Wisam Alshamkhany, Mohamed Mansour, Mueez Khan, Salam Dhou, Fadi Aloul	Decision tree, naïve Bayes, Support vector machine	Decision tree: Accuracy: 99.89 precision: 100 recall: 100 F1-score: 100 Naïve Bayes: Accuracy: 96.90 precision :97 recall :97 F-score:97 SVM: Accuracy: 98.80 precision: 99 recall: 99 F-score :82
Hybrid rule-based botnet detection approach using machine learning for analysing DNS traffic [5]	Saif Al-mashhadi, Mohammed Anbar , Iznan Hasbullah and Taief Alaa Alamiedy	PART and JRip algorithm	Accuracy: 99.96 False positive rate: 1.6 Precision: 99.97 F1 score: 99.97
EKNIS: Ensemble of KNN, Naïve Bayes Kernel and ID3 for Efficient Botnet Classification Using Stacking [6]	Niranjan A, Akshobhya K M, P Deepa Shenoy and Venugopal K R	KNN, Naïve Bayes Kernel and ID3	Accuracy: 99.98 F1-score: 99.99 Precision: 99.99 Recall: 100
Botnet Detection Approach for the Distributed	Oleg Savenko , Anatoliy Sachenko , Sergii Lysenko, and George	Naïve Bayes	Accuracy: 88 FPR: 11.7

Systems [7]	Markowsky		
A Botnet Detection Approach Based on the Clonal Selection Algorithm [8]	Sergii Ly Senko , Kira Bobr ovnikova ,Oleg Savenko	Clonal selection algorithm	Accuracy: 95 False positive rate: 7
Peer to Peer Botnet Detection Using Data Mining Scheme[9]	Wen-Hwa Liao, Chia-Ching Chang	J48,Naïve Bayes, BayesNet	J48: Accuracy: 98 Naïve Bayes: Accuracy: 89 BayesNet: Accuracy: 87
Botnet analysis using ensemble classifier [10]	Anchit Bijalwan , Nanak Chand , Emmanuel Shubhakar Pilli , C. Rama	Ensemble of KNN and decision tree algorithm	Accuracy: 96.41
Detecting IoT Botnets on IoT Edge Devices [11]	Meghana Raghavendra, Zesheng Chen	IPR algorithm and decision tree	Accuracy: 99
Automated Botnet Traffic Detection via Machine Learning [12]	Fok Kar Wai, Zheng Lilei, Watt Kwong Wai, Su Le, Vrizlynn L. L. Thing	Decision tree	Recall: 89.6 FPR: 1.1
Intrusion Detection System for IOT Botnet Attacks Using Deep Learning[13]	Ithu P, Jishma Shareena, Aiswarya Ramdas & Haripriya A P	Naive- Bayes, SVM, decision tree, random forest	Accuracy: 93 Precision: 94 Recall: 90 F1-score: 92
Android botnet detection using signature data and Ensemble Machine Learning. [14]	Viraj Kudtarkar	Decision tree, Random forest , Naive bayes , KNN , Support vector machine	Accuracy: 95.8 Precision: 98.69 Recall: 86.59 F- Measure:92.24
Mobile Botnet Detection: A Deep Learning Approach Using Convolutional Neural Networks.[15]	Suleiman Y. Yerima and Mohammed K. Alzaylaee	Naïve Bayes, SVM, rest, ANN, CNN, j48	CNN (high accuracy): ACC: 98.9 Precision: 98.3 Recall: 97.8 F1score: 98.1
Botnet detection approach using graph-based machine learning [16]	Afnan alharbi, ,Khalid alsubhi	Naïve bayes, decision tree, random forest, adaboost, KNN, Extra Trees	Accuracy: 99 F1-score: 100 Precision: 100 Recall:100
An Ensemble Intrusion Detection Technique	Nour Moustafa, Benjamin Turnbull,	Decision tree, Naïve Bayes , Artificial neural	UNSW-NB15 dataset: HTTP data source: Accuracy: 98.97

based on proposed Statistical Flow Features for Protecting Network Traffic of Internet of Things [17]	Kim-Kwang Raymond Choo,	network	Detection rate: 97.02 False positive rate: 2.58 DNS data source: Accuracy: 99.54 Detection rate: 98.93 False positive rate: 1.38
Effective Botnet Detection Through Neural Networks on Convolutional Features [18]	Shao-Chien Chen, Yi-Ruei Chen, and Wen-Guey Tzeng	Artificial neural network, convolutional neural network	Accuracy: 98.16 False positive rate: 0.5
Botnet Detection with Deep Neural Networks Using Feature Fusion [19]	Chengjie Li, Yunchun Zhang, Wangwang Wang, Zikun Liao, Fan Feng	Deep neural network	Accuracy: 94.78%
BotEye: Botnet Detection Technique Via Traffic Flow Analysis Using Machine Learning Classifiers [20]	Jagdish Yadav, Jawahar Thakur	Random Forest, Ada boost, Decision tree	Accuracy: 98.5 Precision: 99 Recall: 98.8 FPR :2.5
Unsupervised Anomaly Based Botnet Detection in IoT Networks [21]	Sven Nõmm, Hayretdin Bahşi	Clustering algorithm, Self-Organizing Map (SOM), Local Outlier Factor (LOF) and K-NN outlier, Support Vector Machine (SVM)	**Unbalanced Dist.** Accuracy: 93.15 Precision: 96.27 Accuracy: 92.33 Precision: 91.99 Accuracy: 88.27 Precision:88.25 **Balanced Dist.** Accuracy: 83.37 Precision: 76.86 Accuracy: 67.65 Precision: 60.72 Accuracy: 50.50 Precision:50.25
A Visualized Botnet Detection System based Deep Learning for the Internet of Things Networks of Smart Cities [22]	R. Vinayakumar, Mamoun Alazab, Sriram Srinivasan, Quoc-Viet Pham, Soman Kotti Padannayil, K. Simran	Hidden Markov Model (HMM), DT, Support Vector Machine (SVM), Recurrent SVM, LSTM, CNN-LSTM, Bidirectional LSTM, and Extreme learning machine for DGA analysis	RNN: Accuracy: 97.90 Precision: 68.80 Recall: 94.44 F1- Score: 79.60 LSTM: Accuracy: 98.80 Precision: 79.70 Recall: 96.60 F1- Score: 87.10 GRU: Accuracy: 98.70 Precision: 79.10 Recall: 94.60 F1- Score: 86.12

Comparative Study of Botnet Detection System using Different Machine Learning Algorithms [23]	Sharwari Marathe , Prof.Monali Shetty	Logistic Regression, K-Nearest Neighbor, Decision Tree,	KNN: Accuracy: 96.24 Decision Tree: Accuracy: 99.91 Logistic regression: Accuracy: 96.24
Botnet and P2P Botnet Detection Strategies: A Review[24]	H. Dhayal and J. Kumar	Artificial Neural Networks (ANNs), Support Vector Machines (SVM)	Accuracy: 98.1% Precision: 88% Recall: 92% FPR: 0.8%
Machine learning approaches for P2P botnet detection using signal processing technique.[25]	Chittaranjan Hota, Pratik Narang,Vansh Khurana	KNN, REP tree, ANN, SVM	Precision FP-Rate Recall KNN: 0.694 0.041 0.842 REP: 0.985 0.002 0.995 ANN: 0.824 0.02 0.871 SVM: 1 0 0.358
Robust Early-Stage Botnet Detection using Machine Learning[26]	A muhammad, M asad, AR javed	Naive Bayes, Decision tree and ANN	Accuracy: 99 TPR: 99 FPR: 0.7
Botnet detection using recurrent variational auto encoder[27]	Jeeyung Kim, Alex Sim, Jinoh Kim, Kesheng Wu	RVAE, VAE, Random Forest	RVAE: Recall: 0.969 Precision: 0.892 F-Score: 0.929 VAE: Recall: 0.944 Precision: 0.891 F-Score: 0.917 RF: Recall: 0.424 Precision: 0.982 F-Score: 0.592
Botnet forensic analysis using machine learning[28]	Anchit Bijalwan	Decision tree, KNN, Support vector machine, DT-ADA-Boost, Bagging DT, Bagging KNN, Voting DT SVM, Voting SVM KNN	Accuracy Precision Recall F-Score DT (93.70 92.09 94.76) KNN (94.65 95 95 95) SVM (75.99 81.07 76.05 66.78) DT-ADA-Boost (98.36 98.85 98.23 98.54) Bagging DT (95.30 95.25 95.48 95.76) Bagging KNN (94.77 94.89 95 94.42) Voting DT SVM (85.06 87 85 83) Voting SVM KNN (94.65 95 95 95)
Big-data analysis framework for peer-2-peer botnet detection using random forest and deep learning[29]	Abhishek Thakur, Chittaranjan Hota, Kamaldeep Singh, Shardha Guntuku	Random forest, Multi-layer forward neural network	Accuracy RF: 90.30 ML-FNN: 98.41
A P2P botnet detection scheme based on decision tree and adaptive multilayer neural network.[30]	Mohammad Alauthaman, Numan Aslam, Li Zhang, Rafe Alasem, M A Hossain	Bayesian network, Naïve Bayes, J48	Accuracy Bayesian network: 87 Naïve Bayes: 89 J48: 98

Important features that distinguish between benign and anomalous traffic for IoT devices. But it prefers the decision tree as it is simple and gives more accuracy.This paper [12] proposes to use machine learning techniques like multilayer perceptron's and decision trees on network traffic analysis to detect botnet traffic.

[13] A largely extensible Deep Neural Network (DNN) is developed for IoT networks able of willful discovery of the IoT botnet attacks. The evaluation shows that our DNN outperforms the being systems with high delicacy and perfection.

In this paper [14], the researcher suggested a two-layered method for identifying android botnets that combines static analysis with ensemble machine learning at the second layer and signature-based identification at the first layer. With the Logistic Regression classifier, the accuracy achieved is 95.4%. After combining the top three algorithms, this accuracy was significantly increased to 95.8%.

In this research [15], a deep learning model for Android botnet detection based on 1D CNN. Through thorough testing using 1,929 botnet apps and 4,387 clean apps, evaluation of the model. Comparing our CNN-based technique to other well-known machine learning classifiers, the findings demonstrate that it had the highest overall prediction accuracy.

In this paper [16], using the graph-based ML model for detection of botnet.CTU-13 and IoT-23 are two heterogeneous datasets were used for evaluating the effectiveness of the proposed graph-based botnet detection with several ML algorithms. All algorithms were able to successfully detect all bots with 100% recall on both datasets. ExtraTress gives best accuracy between 99% and 100%. IoT plays a vital role in our daily routine life. There is possibility of cyber threats against IoT devices and services. Attackers may attempt to exploit vulnerabilities in application protocols, including Domain Name System (DNS), Hyper Text Transfer Protocol (HTTP) etc. It results in data leakage and security breaches. In this paper [17], using ensemble detection method to mitigate cyber-attacks. an AdaBoost ensemble learning method is developed using Decision tree, artificial neural network, naïve bayes.

The proposed [18] botnet detection system detects P2P botnets more effectively. Our model trains a classification model using a feed-forward artificial neural network. The Experiments show that the accuracy of detection using the convolutional features is better than the ones using the traditional features. Training of the model using convolutional neural network (CNN). It gives high accuracy with low false positive rate.

In this paper [19], introducing the new algorithm for the detection of botnet i.e., neurofuzzy classification techniques. The system achieved an accuracy of 94.78% with 15,000 instances and 56 attributes. Attacks on cloud have been performed to generates the required dataset.

In this paper [20], BotEye is proposed that is a botnet detection technique based on the traffic flow behavior of the network. This technique detects the encrypted botnets also. using CTU-13 dataset with three classifiers namely – Random Forest, ada boost, decision tree. According to the proposed method, the precaptured pcap files are used to calculate the specified features over constant time intervals.

In this paper [21], showing that it is possible to induce high accurate unsupervised learning models with reduced feature set sizes, which enables to decrease the required computational resources. Training one common model for all IoT devices, instead of dedicated model for each device, is another design option that is evaluated for resource optimization.

This paper [22] proposes a botnet detection system based on a two-level deep learning framework for semantically discriminating botnets and legitimate behaviors at the application layer of the domain name system (DNS) services. Embedding features. The experimental results revealed substantial improvements in terms of F1score, speed of detection and false alarm rate.

The author of this paper [23] suggests developing a system for identifying prospective botnets by examining their Internet traffic flows. This system can be installed on a server or a network. The classification model is then constructed using the behavior patterns that are retrieved from the groups of traffic flows that are classified as being similar to each other. To train the model, using bidirectional NetFlow files. The objective of the NetFlow protocol is to gather IP traffic data and track network traffic to get a clearer picture of the network traffic flow. Creating a system that uses machine learning to categorize the flow of botnets. The dataset was subjected to different classifiers.

In this paper [24], a comprehensive review of botnets, their lifecycle and types. Discussion of the peer-to-peer botnet detection techniques' behaviors using various latest detection technique.

[25] KNN and ANN have good precision and recall above 92% and overall precision and recall with SVM is 88%.

This paper [26] proposes an approach for early-stage botnet detection. The approach proposed at first selects the best feature using feature selection techniques. These traits are then fed into a machine learning classifier to evaluate the performance of botnet detection. Experiment shows that the proposed approach efficiently classifies normal and malicious traffic at an early stage. The proposed approach achieves 99% accuracy, true positive rate (TPR) of 0.99%, and false positive rate (FPR) of 0.007%, providing efficient detection rate.

[27] Capture the periodicity within data network, which is key to detect various classes of botnet in dataset.

It [28] uses single classifier and ensemble classifier for detecting botnets. Ensemble classifier gives more accuracy than single classifier.

[29] Uses RF and ML-FNN to detect botnets. RF decrease in accuracy as tree grows larger. This tends to complexity of data and avoided by ML-FNN

[30] Joint classification and regression tree algorithm and neural network have been presented to detect P2P botnet connections.

4. Conclusion

This paper presents and analyzes data from various journal articles and discusses parameters for botnet detection system. Since there are different algorithms already in place to detect bots from a data set or the system. Study about various algorithms that are being used for detecting botnets in dataset. This paper gives us idea about various algorithms used and also about their results. The parameters (accuracy, precision, recall, f-score) give us different results with respect to the algorithm used for the dataset in a particular system. The parameter differs from system-to-system.

5. References

[1] Kuan-Cheng Lin, Sih-Yang Chen, Jason C. Hung, "Botnet Detection Using Support Vector Machines with Artificial Fish Swarm Algorithm", Journal of Applied Mathematics, vol. 2014, Article ID 986428, 9 pages, 2014. https://doi.org/10.1155/2014/986428

[2] Wang, Kuochen & Huang, Chun-Ying & Lin, Shang-Jyh & Lin, Y.R.. (2011). A fuzzy pattern-based filtering algorithm for botnet detection. Computer Networks. 55. 3275-3286.10.1016/j.comnet.2011.05.026.

[3] Mahardhika, Yesta & Sudarsono, Amang & Barakbah, Ali. (2017). An implementation of Botnet dataset to predict accuracy based on network flow model. 33-39. 10.1109/KCIC.2017.8228455.

[4] M. Alshamkhany, W. Alshamkhany, M. Mansour, M. Khan, S. Dhou and F. Aloul, "Botnet Attack Detection using Machine Learning," 2020 14th International Conference on Innovations in Information Technology (IIT), 2020, pp. 203-208, doi: 10.1109/IIT50501.2020.9299061.

[5] Al-mashhadi S, Anbar M, Hasbullah I, Alamiedy TA. 2021. Hybrid rule-based botnet detection approach using machine learning for analysing DNS traffic. PeerJ Computer Science 7: e640 https://doi.org/10.7717/peerj-cs.640

[6] Appaswamy, Niranjan & M., Akshobhya & Shenoy, P. & K R, Venugopal. (2018). EKNIS: Ensemble of KNN, Naïve Bayes Kernel and ID3 for Efficient Botnet Classification Using Stacking. 1-6. 10.1109/ICDSE.2018.8527791.

[7] O. Savenko, A. Sachenko, S. Lysenko and G. Markowsky, "Botnet Detection Approach for the Distributed Systems," 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 2019, pp. 406-411, doi: 10.1109/IDAACS.2019.8924428.

[8] S. Lysenko, K. Bobrovnikova and O. Savenko, "A botnet detection approach based on the clonal selection algorithm," 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), 2018, pp. 424-428, doi: 10.1109/DESSERT.2018.8409171.

[9] W. -H. Liao and C. -C. Chang, "Peer to Peer Botnet Detection Using Data Mining Scheme," 2010 International Conference on Internet Technology and Applications, 2010, pp. 1-4, doi: 10.1109/ITAPP.2010.5566407.

[10] Anchit Bijalwan, "Botnet Forensic Analysis Using Machine Learning", Security and Communication Networks, vol. 2020, Article ID 9302318, 9 pages, 2020. https://doi.org/10.1155/2020/9302318

[11] M. Raghavendra and Z. Chen, "Detecting IoT Botnets on IoT Edge Devices," 2022 IEEE International Conference on Communications Workshops (ICC Workshops), 2022, pp. 373-378, doi: 10.1109/ICCWorkshops53468.2022.9814555.

[12] F. K. Wai, Z. Lilei, W. K. Wai, S. Le and V. L. L. Thing, "Automated Botnet Traffic Detection via Machine Learning," TENCON 2018 - 2018 IEEE Region 10 Conference, 2018, pp. 0038-0043, doi: 10.1109/TENCON.2018.8650466.

[13] P, J., Shareena, J., Ramdas, A. et al. Intrusion Detection System for IOT Botnet Attacks Using Deep Learning. SN COMPUT. SCI. 2, 205 (2021). https://doi.org/10.1007/s42979-021-00516-9

[14] D. Zhuang and J. M. Chang, "Enhanced PeerHunter: Detecting Peer-to-Peer Botnets Through Network-Flow Level Community Behavior Analysis," in IEEE

Transactions on Information Forensics and Security, vol. 14, no. 6, pp. 1485-1500, June 2019, doi: 10.1109/TIFS.2018.2881657.

[15] D. Nanthiya, P. Keerthika, S. B. Gopal, S. B. Kayalvizhi, T. Raja and R. S. Priya, "SVM Based DDoS Attack Detection in IoT Using Iot-23 Botnet Dataset," 2021 Innovations in Power and Advanced Computing Technologies (i-PACT), 2021, pp. 1-7, doi: 10.1109/i-PACT52855.2021.9696569.

[16] A. Alharbi and K. Alsubhi, "Botnet Detection Approach Using Graph-Based Machine Learning," in IEEE Access, vol. 9, pp. 99166-99180, 2021, doi: 10.1109/ACCESS.2021.3094183.

[17] N. Moustafa, B. Turnbull and K. -K. R. Choo, "An Ensemble Intrusion Detection Technique Based on Proposed Statistical Flow Features for Protecting Network Traffic of Internet of Things," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4815-4830, June 2019, doi: 10.1109/JIOT.2018.2871719.

[18]] S. -C. Chen, Y. -R. Chen and W. -G. Tzeng, "Effective Botnet Detection Through Neural Networks on Convolutional Features," 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), 2018, pp. 372-378, doi: 10.1109/TrustCom/BigDataSE.2018.00062.

[19] C. Li, Y. Zhang, W. Wang, Z. Liao and F. Feng, "Botnet Detection with Deep Neural Networks Using Feature Fusion," 2022 International Seminar on Computer Science and Engineering Technology (SCSET), 2022, pp. 255-258, doi: 10.1109/SCSET55041.2022.00066.

[20] J. Yadav and J. Thakur, "BotEye: Botnet Detection Technique Via Traffic Flow Analysis Using Machine Learning Classifiers," 2020 Sixth International Conference on Parallel, Distributed and Grid Computing (PDGC), 2020, pp. 154-159, doi: 10.1109/PDGC50313.2020.9315792.

[21] S. Nõmm and H. Bahşi, "Unsupervised Anomaly Based Botnet Detection in IoT Networks," 2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA), 2018, pp. 1048-1053, doi: 10.1109/ICMLA.2018.00171.

[22] R. Vinayakumar, M. Alazab, S. Srinivasan, Q. -V. Pham, S. K. Padannayil and K. Simran, "A Visualized Botnet Detection System Based Deep Learning for the Internet of Things Networks of Smart Cities," in IEEE Transactions on Industry Applications, vol. 56, no. 4, pp. 4436-4456, July-Aug. 2020, doi: 10.1109/TIA.2020.2971952.

[23] Marathe, S. and Shetty, M., Comparative Study of Botnet Detection System using Different Machine-Learning Algorithms.

[24] H. Dhayal and J. Kumar, "Botnet and P2P Botnet Detection Strategies: A Review," 2018 International Conference on Communication and Signal Processing (ICCSP), 2018, pp. 1077-1082, doi: 10.1109/ICCSP.2018.8524529.

[25] Pratik Narang, Vansh Khurana, and Chittaranjan Hota. 2014. Machine-learning approaches for P2P botnet detection using signal-processing techniques. In Proceedings of the 8th ACM International Conference on Distributed Event-Based Systems (DEBS '14). Association for Computing Machinery, New York, NY, USA, 338–341

[26] A. Muhammad, M. Asad and A. R. Javed, "Robust Early Stage Botnet Detection using Machine Learning," 2020 International Conference on Cyber Warfare and Security (ICCWS), 2020, pp. 1-6, doi: 10.1109/ICCWS48432.2020.9292395.

[27] J. Kim, A. Sim, J. Kim and K. Wu, "Botnet Detection Using Recurrent Variational Autoencoder," GLOBECOM 2020 - 2020 IEEE Global Communications Conference, 2020, pp. 1-6, doi: 10.1109/GLOBECOM42002.2020.9348169

[28] Anchit Bijalwan, "Botnet Forensic Analysis Using Machine Learning", Security and Communication Networks, vol. 2020, Article ID 9302318, 9 pages, 2020.

[29] Kothandapani, Vijayaprabakaran. (2019). Big Data Analytics Framework for Peer-To-Peer Botnet Detection Using Random Forest and Deep Learning. International Journal of Computer Science and Information Security, 15. 269-277.

[30] Alauthaman, M., Aslam, N., Zhang, L. et al. A P2P Botnet detection scheme based on decision tree and adaptive multilayer neural networks. Neural Comput & Applic 29, 991–1004 (2018).