International Journal of Innovative Research in Engineering & Management (IJIREM)
ISSN: 2350-0557, Volume-9, Issue-4, August 2022
https://doi.org/10.55524/ijirem.2022.9.4.1
Article ID IJIRD-1183, Pages 1-5
www.ijirem.org

A Cloud Based Machine Intelligent Framework to Identify DDoS Botnet Attack in Internet of Things

Sourav Kumar Bhoi[1], and Krishna Prasad K[2]

[1] Post Doctoral Fellow, Research Center Department, Computer Science and Information Science,
Institute of Computer Science and Information Science, Srinivas University, Mangaluru-575001, Karnataka, India
[2] Associate Professor, Institute of Computer Science and Information Science, Srinivas University, Pandeshwar, Mangaluru, Karnataka, India

Correspondence should be addressed to Sourav Kumar Bhoi; skbhoi300@gmail.com

ABSTRACT- First few Botnet attack is a major issue in security of Internet of Things (IoT) devices and it needs to be identified to secure the system from the attackers. In this paper, a cloud-based machine intelligent framework is proposed to identify DDoS (distributed denial of service) Botnet attack in IoT systems. In this framework, the IoT devices communicating with the cloud are categorized based on their communication record to check the DDoS Botnet attack. In this work, three DDoS botnet attacks are considered such as HTTP, UDP, and TCP. The cloud is installed with a supervised machine intelligent model to classify the type of DDoS attack. The model is selected by considering 4 models such as Tree, stacking classifier, Neural Network (NN), and Support Vector Machine (SVM) and performance is evaluated based on classification accuracy (CA). Here, the stacking classifier is a hybrid model designed using the aggregation of Logistic Regression (LR), NN, and SVM. The performance is evaluated using Python tool. From the results it was found that except Tree all three models show an CA of 1.0. The computation time is also analyzed for four models and it was found that Tree shows less time than other models however, if considered with respect to CA (1.0) then SVM can be preferred as it shows lesser time then other two models. The detection time of the IoT devices is also simulated and result show that if SVM is installed in cloud then the detection time is lesser.

KEYWORDS- Security, DDoS Botnet Attack, IoTs, Supervised Machine Learning, Classification Accuracy

I. INTRODUCTION

Security is now a major concern in IoT Systems. IoT is a network where any device with sensors and Internet are connected to each other using wireless or wired communication to perform a task [1,2]. For any task processing, the data communication is needed between any two devices. If a device is communicating with other device, then the data should be secured or the device with which communication is going on should be a genuine user means it should not be an attacker. As IoT has many real time applications for the users, the data transmitted should be correct and accurate. So, security is a need in this context to detect the IoT devices very accurately as genuine user or attacker. Such an attack is DDoS attack where the attacker controls the whole network by flooding the packets to the network/any device for service disruption [3-5]. The device or network will be jammed with packet processing and it is unable to give services on request or gives service in delay. DDoS has many types of attack, however in this work we focus on DDoS Botnet attack. Botnet attack is an attack where the attacker controls the whole network of devices and each device now acts under the control of the attacker as a bot [3-16]. These devices are then instructed by the attacker to flood the packets to perform service disruption. So, this needs to be detected after a communication happened. For detection of attacker very accurately, nowadays machine learning is a very demanding approach in AI (artificial intelligence). Machine learning [17-20] mainly solves many types of problems such as classification, prediction, recognition, clustering, etc. So, in this work, we consider in classification problem where the IoT devices which acts as attackers flood UDP/TCP/HTTP packets in the network and these subcategories needs to be detected very accurately with a best machine learning model.

The main contributions in this work are represented as follows:

- In this work, a cloud-based machine intelligent framework is proposed to categorized DDoS Botnet attack in IoT systems.
- In this framework, the IoT devices communicating with the cloud are identified based on their communication record to check the DDoS Botnet attack. Three types of DDoS botnet attacks are considered such as HTTP, UDP, and TCP from Kaggle [21].
- The cloud is installed with a supervised machine intelligent model to classify the type of DDoS attack. The model is selected by considering four models such as Tree, stacking classifier, NN, and SVM. The performance is evaluated based on CA.
- Here, the stacking classifier is a hybrid model designed using the aggregation of LR, NN, and SVM.

- The performance is evaluated using Python tool. From the results it was found that except Tree all three models show an CA of 1.0. The computation time is also analyzed and it was found that Tree shows less computation time than other models, however, if considered with respect to CA of 1.0 then SVM can be preferred as it shows lesser time then other two models.
- The detection time of the IoT devices is also simulated and result show that if SVM is installed in the cloud then the detection time is lesser.

The rest of the sections are described as follows. Section II presents the related work, Section III presents the methodology, Section IV presents the simulation and results, and Section V presents the conclusion and future scope.

II. RELATED WORK

Many such research works are conducted in this area, some are discussed as follows. Kolias et al. [3] studied about the DDoS attack in IoT. Shafi et al. [4] proposed a method using blockchain to prevent DDoS attack in software defined network. Vishwakarma et al. [5] surveys about the defense mechanism for DDoS attack in IoT. De Donno et al. [6] analyzes about the IoT malwares doing DDoS attack. Vishwakarma et al. [7] proposed a honeypot with machine intelligence framework to save the network from DDoS botnet attack. Sareena et al. [8] proposed an IDS using deep learning to detect the DDoS botnet attack. Sriram et al. [11] proposed a network flow based deep learning method to detect the IoT botnet attack. Injadat et al. [12] proposed an optimized machine learning based approach to detect the botnet attack. Soe et al. [13] proposed a sequential architecture to detect the IoT botnet attack. Meidan et al. [14] proposed a deep autoencoders based machine learning approach to detect the IoT botnet attack. Lee et al. [15] proposed a honeypot with machine learning approach to detect machine learning approach in IoT smart factory. From above methods, it was found that cloud based IoT botnet attack classification using machine learning approach is not done. Also, the attacks like HTTP/UDP/TCP are not considered in above works as per our knowledge. Therefore, in this work we have proposed a framework to identify and categorize the type of IoT botnet attack using cloud.

III. PROPOSED FRAMEWORK

The framework mainly consists of a two-tier architecture where the IoT devices are directly connected to the cloud service provider as represented in Fig. 1. The IoT devices communicates with the cloud to get services on demand. The IoT devices can communicate with the cloud using Base Station and Gateway. The cloud also uses this communication channel to communicate with the IoT devices. The device after communication with the cloud is checked by the cloud using the machine intelligence model to detect the type of DDoS botnet attack in the system.

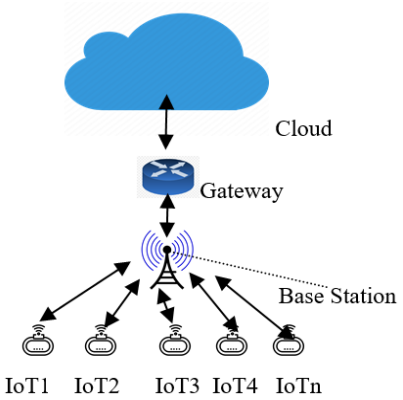

Figure 1: System architecture framework

DDoS Botnet attack is a type of attack where the attacker controls a group of devices in the network by controlling through the compromised controller as represented in Fig. 2. From Fig. 2 it is observed that the IoT devices are connected to the controller that is compromised and the devices can communicate with cloud on demand. Here, the DDoS attacker instructs the IoT devices to flood packets to the cloud unnecessarily to disrupt the cloud service to other users and for controlling the network. The devices can create flooding of different types of DDoS attacks such as HTTP, UDP, and TCP. In this work, we consider these three for detection of DDoS attack in the simulation.

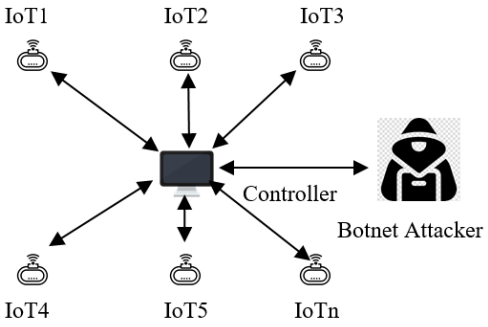

Figure. 2: DDoS Botnet Attack

The steps to detect the DDoS botnet attacker category is represented as follows:

- The IoT device communicates with the cloud.
- After communication the communication record is stored in the local memory of the cloud.
- The cloud then uses the best supervised machine learning model for classifying the record as DDoS botnet attack of category such as HTTP/ UDP/ TCP.
- The best supervised machine learning model is selected using a standard dataset. The dataset is used for training the models (Tree, Stacking Classifier, NN, and SVM) and testing with the model. The model with high classification accuracy is selected a s the best model for the cloud.
- After selection of best model, the model is installed at the cloud for classification of DDoS botnet attack category.

- As communication record is already recorded at cloud for a device after communication, cloud then finds the device DDoS Botnet attack category.
- After finding the DDoS attacker category, the cloud can take necessary action over the malicious IoT device as per the protocol.

IV. SIMULATION AND RESULTS

The performance of the system framework is evaluated using Python tool. The machine in which the simulation is conducted has 8GB RAM, windows 64-bit OS, and has a processor speed of 2.4 GHz. The models taken for this simulation are Tree, Stacking Classifier (STACK), NN and SVM. The stacking classifier or STACK is designed by the aggregation of LR, NN and SVM. The performance metrics taken are AUC (area under curve), CA, F1, Precision and Recall. However, we have considered CA as the main parameter for categorizing the DDoS Botnet attack.

The dataset taken for this simulation is taken from Kaggle data repository [21]. Due to its large size, we have considered only 2988 instances for three attacks of DDoS Botnet attack such as HTTP, TCP, and UDP. HTTP has 988, TCP has 1000 and UDP has 1000 instances of data. The dataset consists of 46 columns or attributes such as packet sequence ID, source port, destination post, source address, destination address, packets, bytes, state, etc. and the last column represent HTTP/TCP/UDP category of attack in the system. Here, in the dataset the IoT devices are communicating with a server assumed as cloud (destination address: 192.168.100.3). The destination is assumed to classify the attacks.

The results are represented in Table 1 and Fig. 7 as follows. From the results it is observed that Tree shows a CA of 0.99, and STACK, NN, and SVM shows CA of 1.0. So, it can be concluded that any of three models can be taken for installation at cloud, however the computation time is also important for selection of best model. So, from Figure 8 it is observed that the computation time for Tree is 1.5 secs, STACK shows 101 secs, NN shows 10.5 secs, and SVM shows 3 secs. So, it is better to consider SVM because it shows CA of 1 and the computation time is also less. Fig. 3 to Fig. 6 shows the confusion matrix of the models. The diagonal matrix shows what number of actuals is correctly predicted.

Table 1: Comparison of Tree, STACK, NN and SVM

Models	AUC	CA	F1	Precision	Recall
TREE	0.99	0.99	0.99	0.99	0.99
STACK	1	1	1	1	1
NN	1	1	1	1	1
SVM	1	1	1	1	1

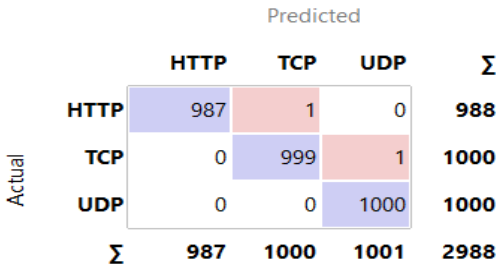

Figure. 3: Confusion matrix of Tree

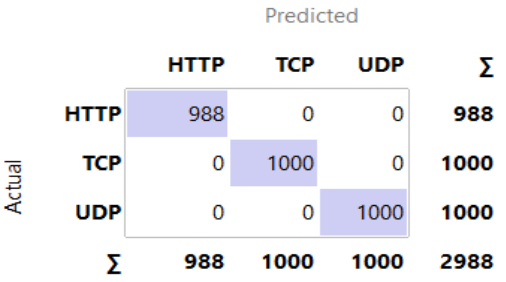

Figure. 4: Confusion matrix of STACK

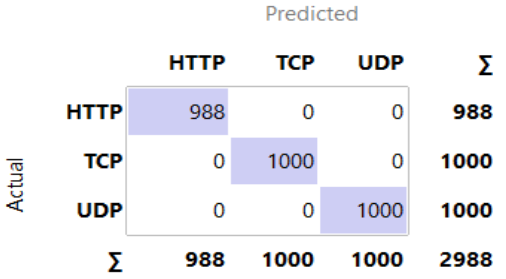

Figure. 5: Confusion matrix of NN

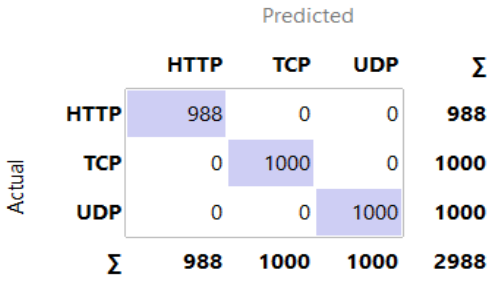

Figure. 6: Confusion matrix of SVM

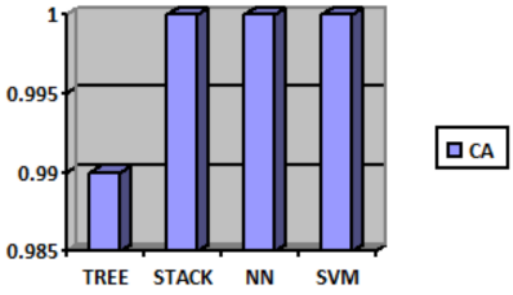

Figure. 7: Comparison of classification accuracy in range 0-1 (y-axis) for different models (x-axis)

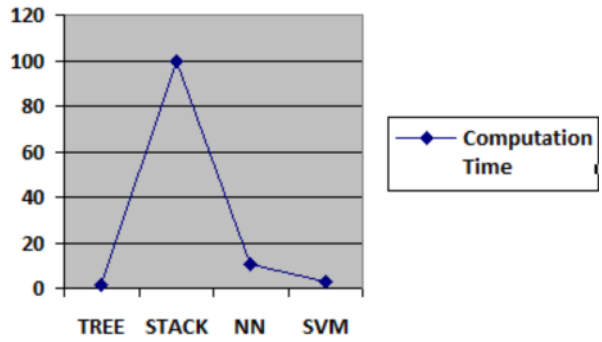

Figure. 8: Comparison of computation time in secs (y-axis) for different models (x-axis)

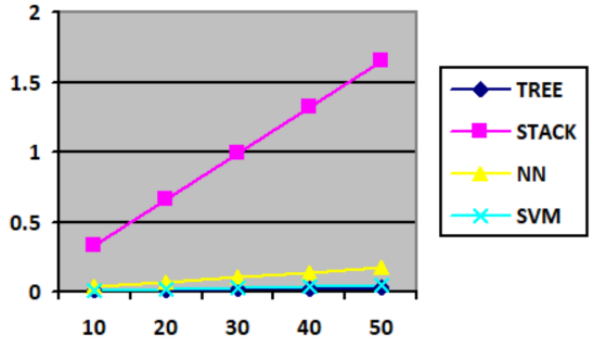

Figure. 9: Comparison of detection time in secs (y-axis) for 10-50 IoT devices (x-axis) for different models

The simulation is also performed for calculation of detection time of attack when the number of IoT devices increases in a network. The simulation setting is shown in Table 2. So, here detection time is defined as the time required to detect the communication record of n number of IoT devices to check or classify the type of DDoS botnet attack. From result it is observed that SVM show better performance of CA as 1 and has less detection time then others. When the IoT devices are 50, SVM show 0.05 secs of detection time whereas NN and STACK show detection time of 0.175 secs and 1.65 secs respectively. So, SVM will be a better machine learning model for our proposed framework. Fig. 9 shows the comparison of detection time for different models when installed at cloud.

Table 2: Simulation settings for Detection time

Sl. no.	Parameter	Value
1	Number of cloud device	1
2	Number of IoT devices connected to cloud	10-50
3	Attack type	DDoS Botnet attack (HTTP, UDP and TCP)
4	Average processing time for a sample for Tree	0.0005sec
5	Average processing time for a sample for Tree	0.033sec
6	Average processing time for a sample for NN	0.0034sec
7	Average processing time for a sample for SVM	0.001sec

V. CONCLUSION

In this work, a cloud-based machine intelligent framework is proposed to categorize the DDoS Botnet attack in IoT systems as HTTP/TCP/UDP. From the results it is observed that Tree shows a CA of 0.99, and STACK, NN, and SVM shows CA of 1.0. So, it can be concluded that any of three models can be taken for installation at cloud, however the computation time is better for SVM showing 3 secs. So, it is better to consider SVM because it shows CA of 1 and the computation time is also less. Further simulation is performed for detection time and SVM shows less detection time than others. When the IoT devices are 50, SVM show 0.05 secs of detection time whereas NN and STACK show detection time of 0.175 secs and 1.65 secs respectively. So, SVM will be a better machine learning model for our proposed framework. In future, we will consider larger dataset with new machine learning models to improve the CA and reduce the detection time at cloud.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

ACKNOWLEDGMENT

Our thanks to Srinivas University, Mangaluru, India for giving facility to conduct this post doctoral research work in the area of security in IoT using machine learning.

REFERENCES

[1] Xu, T., Wendt, J. B., & Potkonjak, M. (2014, November). Security of IoT systems: Design challenges and opportunities. In 2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD) (pp. 417-423). IEEE.

[2] Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. Journal of Information Security and Applications, 38, 8-27.

[3] Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. Computer, 50(7), 80-84.

[4] Shafi, Q., & Basit, A. (2019, January). DDoS botnet prevention using blockchain in software defined internet of things. In 2019 16th international Bhurban conference on applied sciences and technology (IBCAST) (pp. 624-628). IEEE.

[5] Vishwakarma, R., & Jain, A. K. (2020). A survey of DDoS attacking techniques and defence mechanisms in the IoT network. Telecommunication systems, 73(1), 3-25.

[6] De Donno, M., Dragoni, N., Giaretta, A., & Spognardi, A. (2017, September). Analysis of DDoS-capable IoT malwares. In 2017 Federated Conference on Computer Science and Information Systems (FedCSIS) (pp. 807-816). IEEE.

[7] Vishwakarma, R., & Jain, A. K. (2019, April). A honeypot with machine learning based detection framework for defending IoT based botnet DDoS attacks. In 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI) (pp. 1019-1024). IEEE.

[8] Shareena, J., Ramdas, A., & AP, H. (2021). Intrusion detection system for iot botnet attacks using deep learning. SN Computer Science, 2(3), 1-8.

[9] Ali, I., Ahmed, A. I. A., Almogren, A., Raza, M. A., Shah, S. A., Khan, A., & Gani, A. (2020). Systematic literature review on IoT-based botnet attack. IEEE Access, 8, 212220-212232.

[10] Bertino, E., & Islam, N. (2017). Botnets and internet of things security. Computer, 50(2), 76-79.

[11] Sriram, S., Vinayakumar, R., Alazab, M., & Soman, K. P. (2020, July). Network flow based IoT botnet attack detection using deep learning. In IEEE INFOCOM 2020-IEEE conference on computer communications workshops (INFOCOM WKSHPS) (pp. 189-194). IEEE.

[12] Injadat, M., Moubayed, A., & Shami, A. (2020, December). Detecting botnet attacks in IoT environments: an optimized machine learning approach. In 2020 32nd International Conference on Microelectronics (ICM) (pp. 1-4). IEEE.

[13] Soe, Y. N., Feng, Y., Santosa, P. I., Hartanto, R., & Sakurai, K. (2020). Machine learning-based IoT-botnet attack detection with sequential architecture. Sensors, 20(16), 4372.

[14] Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Shabtai, A., Breitenbacher, D., & Elovici, Y. (2018). N-baiot—network-based detection of iot botnet attacks using deep autoencoders. IEEE Pervasive Computing, 17(3), 12-22.

[15] Lee, S., Abdullah, A., Jhanjhi, N., & Kok, S. (2021). Classification of botnet attacks in IoT smart factory using honeypot combined with machine learning. PeerJ Computer Science, 7, e350.

[16] Dange, S., & Chatterjee, M. (2020). IoT botnet: the largest threat to the IoT network. In Data Communication and Networks (pp. 137-157). Springer, Singapore.

[17] Bhoi, S. K., Mallick, C., Mohanty, C. R., & Nayak, R. S. (2022). Analysis of Noise Pollution during Dussehra Festival in Bhubaneswar Smart City in India: A Study Using Machine Intelligence Models. Applied Computational Intelligence and Soft Computing, 2022.

[18] Bhoi, S. K., Mallick, C., & Mohanty, C. R. (2022). Estimating the Water Quality Class of a Major Irrigation Canal in Odisha, India: A Supervised Machine Learning Approach. Nature Environment and Pollution Technology, 21(2), 433-446.

[19] Bhoi, A., Nayak, R. P., Bhoi, S. K., Sethi, S., Panda, S. K., Sahoo, K. S., & Nayyar, A. (2021). IoT-IIRS: Internet of Things based intelligent-irrigation recommendation system using machine learning approach for efficient water usage. PeerJ Computer Science, 7, e578.

[20] Bhoi, S. K. (2021). Prediction of diabetes in females of pima Indian heritage: a complete supervised learning approach. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(10), 3074-3084.

[21] https://www.kaggle.com/datasets/siddharthm1698/ddos-botnet-attack-on-iot-devices?select=DDoSdata.csv, accessed on 24th June 2022.

ABOUT THE AUTHORS

Dr. Sourav Kumar Bhoi is currently pursuing his post doctoral research work as a Post Doctoral Fellow, in Srinivas University, Mangaluru, Karnataka, India. His research interests are Machine Learning and IoT.

Dr. Krishna Prasad K is currently working as Associate Professor in Srinivas University, Mangaluru, Karnataka, India. His research interest includes AI, Biometric Security, Healthcare Data Analysis.