2nd International Conference on Emerging Trends in Materials, Computing and Communication Technologies
International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)

# A Review on Botnet DDOS Attack Detection on IoT Devices Using Machine Learning

**Sahila Devi R[1], Dr.R.Bharathi[2], Dr.P.Krishna kumar[3]**

[1]Department of computer science and Engineering, Rohini College of Engineering and Technology, Tamil Nadu, India

[2]Professor, Department of Electronics and Communication Engineering, University College of Engineering, Konam, Tamil Nadu, India

[3]Professor, Department of Computer Science and Engineering, VV College of Engineering, Tisayanvilai, Tamil Nadu, India

## ABSTRACT

Due to the drastic amount of increase in IOT devices the vulnerability threat against the IOT devices also increases. The Botnet is one of the most important vulnerability threats against IOT devices nowadays. They are the roots for malware, phishing, Distributed Denial of Service Attacks (DDoS), spam. To overcome the problem of DDoS attack, various machine learning methods typically Support Vector Machine (SVM), Artificial Neural Network (ANN), Naïve Bayes (NB), Decision Tree (DT), and Unsupervised Learning (USML) (K-means, X-means, etc.) were proposed. With the drastic increase in usageof Machine Learning in IOT DDoS detection, it will be important to analyze various machine learning algorithms which support DDoS detection on IOT devices. This could help the researchers to choose a suitable machine learning algorithm for DDoS Detection and assist them in future research. This paper performed an analysis on the machine learning methods for Botnet DDoS attack detection.

**Keywords—** IOT, Machine Learning, DDoS,

## I. INTRODUCTION

Internet of Things (IoT) is an enhancing technology which highly assists humans. In today's world, IoT plays a vital role in our lives. IoT is used in smart homes, smart agriculture, smart cities etc.The major goal of IoT technology is to create human life additional manageable and smarter by merging physical devices and digital intelligence[1,2,3,4]

The major vulnerabilities of IoT devices are insecure IoT interfaces due to Weak credentials, Insufficient authentication and authorization because of insecure login credentials and Insecure software and network services, malware distribution due to Weak physical security Ports, SD cards and storage media etc.

The security threats to IoT devices and networks can be sorted into different categories

- DoS attackers: The attackers flood the target server with superfluous requests to forestall IoT devices from getting services . one of the foremost dangerous forms of a DoS attack is once DDoS attackers use thousands of net protocol addresses to request IoT services, creating it troublesome for the server to differentiate the legitimate IoT devices from attackers. Distributed IoT devices with lightweight security protocols square measure particularly prone to DDoS attacks.
- Jamming: Attackers interrupt the continuing radio transmissions of IoT devices by sending fake signals and reduce the bandwidth, central process units (CPUs), and memory resources of IoT devices or sensors throughout their unsuccessful communication attempts .
- Spoofing: A spoofing node imitates a legal IoT device with its identities like the MAC address and RFID tag to achieve extrajudicial access to the IoT system and may launch attacks like DoS and manin-the-middle attacks .
- Man-in-the-middle attack: A man-in-the-middle attacker sends signals which jam and spoof with the goal of covertly monitoring, spying, and modifying the private communication between IoT devices [4].
- Software attacks: Mobile malware like Trojans, worms, and viruses may end up in privacy outflow, economic loss, power depletion, and network performance degradation of IoT systems [6].
- Privacy leakage: IoT systems need to defend user privacy throughout information caching and exchange. Some caching vendors are keen on keeping the data contained on their devices and analyzing and selling such IoT privacy information. Wearable devices that collect users' personal data like location and personal data on ailments have witnessed an augmented risk of private privacy outflow.

## II. ABOUT DDOS ATTACK

The main goal of a DDoS hacker is to control the IoT devices in the network to change them into a zombie army. A DDoS attack is giant enough to bring even a "secure" company network down, or it is small—barely noticeable "white noise" that escapes human detection nevertheless infiltrates and maps networks in a very matter of seconds.

### Machine learning methods related to DDoS attack detection

Signature-based IDS is a human-handed operation, involving several hours of testing, developing and deploying the signature, and making new signatures for unknown attacks too. Therefore, providing a less human-based system is made essential. Machine Learning languages derived anomaly-based IDS offers an answer to the present issue, serving to include a framework that might learn from information and predict unknown stats data on learned information.

- **Naïve Bayes**

Naive Bayes is targetted on the Bayesian classification model. Establishing classifiers is an effortless and straightforward method: prototypes that give class labels to issue cases, defined as the vectors of showcasing values, in which the classes labels will be taken from a fixed set.

- **Support Vector Machine Support Vector Machine (SVM)**

SVM makes classification and regression using the regulated method of learning. Based on a group of trained examples, each of which is shown as methods are divided into two categories, an SVM algorithm creates a design that foresees that the new instance tends to fall into one among the two.

- **Decision Trees**

One of the fundamental techniques utilized in machine learning and data processing is the decision tree. It is also utilized as a prognostic model where findings regarding an object are mapped to assumptions about the preferred value of the item. A decision tree may be used in the decision data analysis to indicate decision making graphically and clearly. The data set is analyzed and built-in this method. Therefore, if the new data element is offered for categorization, the prior dataset will categorize it properly. DOS attacks can be detected using Decision Trees.

- **K-means clustering**

It is a clustering technique commonly used to divide a set of data into groups. The K-means clustering algorithm runs by selecting k initial cluster centers in a data set and later refining them repeatedly as describes

1. Each example will be allotted to its closest cluster core.
2. It updates the mean of its elements to each of the cluster centers. The algorithm joins when the allocation of requests to clusters performs not further and then compares it with the alternative rule-based algorithms, such as the Decision table.

- **AdaBoost**

Adaptive Boosting algorithm is an ensemble learning algorithm that understands weak algorithms' flaws and attempts to improve them and also make them robust classifiers progressively. In each iteration, the classifier becomes improves itself, which is its primary benefit over arbitrary predictions.

- **XGBoost**

Xtreme Gradient Boosting is a categorization algorithm that attempts to boost the model's precision by reducing the error in every iteration

- **KNN:**

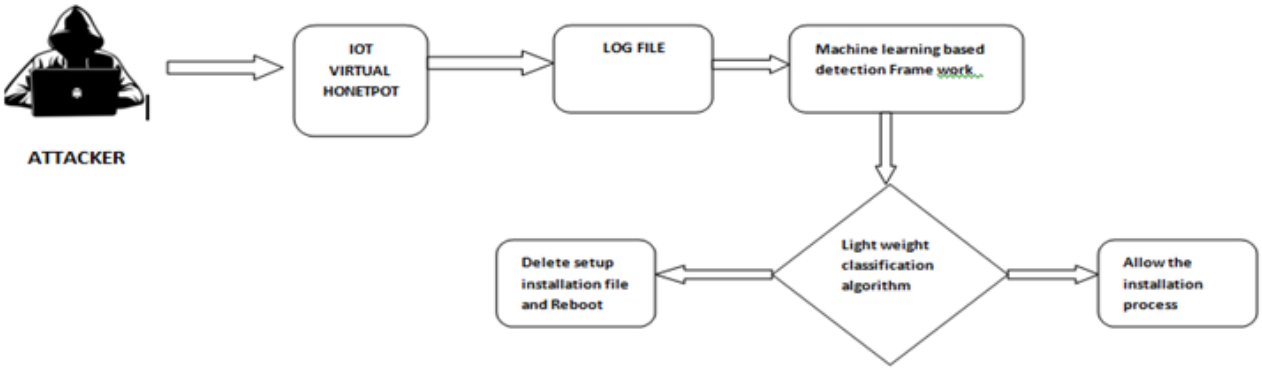
K-Nearest Neighbors is a managed classification algorithm that uses k-closest training examples as input.

- **Random Forest**

It is a collective learning method for categorization, and it comprises a set of decision trees that are arbitrarily selected for training; and in the end, the ultimate vote will be the outcome of all these trees.

## III. COMPARISION

- Smart Detection :An online approach for DOS/DDoS attack detection using machine learning [7]
  To classify the network traffic this paper uses random forest tree algorithm. It works based on samples taken by the sFlow protocol directly from network devices .It creates inferences based on the signature that was previously extracted from samples of network traffic.
- A honey pot with machine learning based detection frame work for defending IOT based botnet DDos Attack [10]
  This paper uses a honeypot based approach. The honeypots use machine learning techniques for malware detection. The IoT honeypot generated data is used as a dataset for effective and dynamic training of machine learning models.




- Cluster based semi-supervised machine learning for DDoS attack classification[8]
  In this approach the unlabelled traffic which includes traffic rate , processing delay and CPU utilization are clustered by two clustering algorithms namely agglomerative clustering algorithm and K-mean clustering algorithms ,the results of these clustering algorithms are given as an input to the voting system. The voting system decides the final labelling of traffic flow.
- Boosting-based DDoS Detection in Internet of Things Systems[11]
  DDoS traffic detection model uses a boosting method of logistic model trees for different IoT device classes.Example Class 1 – very high level of traffic predictability, Class 2 – high level of traffic predictability, Class 3 – medium level of traffic predictability, and Class 4 – low level of traffic predictability. Based on the variation of traffic flow compared with the regular flow the system detect the device's abnormal behavior.
- A Supervised Intrusion Detection System for Smart Home IoT Devices[12]
  This paper proposes an Intrusion Detection System (IDS) that uses three-layer approach, that uses a supervised approach to detect a variety of network-based cyber-attacks on IoT networks. This system uses three main steps: first, it classifies the type and log the normal behavior of each IoT device that is connected to the network, In the second step it identifies the malicious packets on the network when an attack is happening Finally it classifies the type of the attack.

## IV. REFERENCES


[1]. H. Tyagi and R. Kumar, "Attack and Anomaly Detection in IoT Networks Using Supervised Machine Learning Approaches," Rev. d'Intelligence Artif., vol. 35, no. 1, pp. 11-21, 2021.

[2]. S. Kaur, J. Singh, and K. K. A. S. GCET, "Attack Detection Using Machine Learning Approach."

[3]. J. Li, Z. Xue, C. Li, and M. Liu, "RTED-SD: A Real-Time Edge Detection Scheme for Sybil DDoS on the Internet of Vehicles," IEEE Access, vol. 9, pp. 11296-11305, 2021.

[4]. N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network intrusion detection for IoT security based on learning techniques," IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2671-2701, 2019.

[5]. S. Pokhrel, R. Abbas, and B. Aryal, "IoT Security: Botnet detection in IoT using Machine learning," arXiv preprint arXiv:2104.02231, 2021.

[6]. K. Wehbi, L. Hong, T. Al-salah and A. A. Bhutta, "A Survey on Machine Learning Based Detection on DDoS Attacks for IoT Systems," 2019 SoutheastCon, 2019, pp. 1-6, doi: 10.1109/SoutheastCon42311.2019.9020468.

[7]. Francisco Sales de Lima Filho" Smart Detection: An Online Approach for DoS/DDoS Attack Detection Using Machine Learning" olume 2019 |ArticleID 1574749 | https://doi.org/10.1155/2019/1574749

[8]. MuhammadAamirSyed MustafaAli Zaidi"Clustering based semi-supervised machine learning for DDoS attack classification" Journal of King Saud University - Computer and Information SciencesVolume 33, Issue 4, May 2021, Pages 436-446

[9]. X. Li, R. Lu, X. Liang, and X. Shen, "Smart community: An Internet of things application," IEEE Commun. Mag., vol. 49, no. 11, pp. 68–75, Nov. 2011.

[10]. R. Vishwakarma and A. K. Jain, "A Honeypot with Machine Learning based Detection Framework for defending IoT based Botnet DDoS Attacks," 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), 2019, pp. 1019-1024, doi: 10.1109/ICOEI.2019.8862720

[11]. Ivan Cvitic, Dragan Perakovic, Brij Gupta, Kim-Kwang Raymond Choo" Boosting-based DDoS Detection in Internet of Things Systems." ISSN 2327-4662

[12]. E. Anthi, L. Williams, M. Słowińska, G. Theodorakopoulos and P. Burnap, "A Supervised Intrusion Detection System for Smart Home IoT Devices," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 9042-9053, Oct. 2019, doi: 10.1109/JIOT.2019.2926365.