MACHINE LEARNING AND DEEP LEARNING MODEL-BASED DETECTION OF IOT BOTNET ATTACKS.

Anuja Lakhe[1], Sunilkumar Jaiswal[2]

M.tech, Department of Computer Science and Engineering, MGM university, Jawaharlal Nehru Engineering College, Aurangabad, India
Assistant Professor, Department of Computer Science and Engineering, MGM university, Jawaharlal Nehru Engineering College, Aurangabad, India

---***---

Abstract- *Computers and networks have been under threat from viruses, worms, and attacks from hackers since they were first used. In 2018, the number of devices connected to the Internet exceeded the number of human beings and this increasing trend will see about 80 billion devices by 2024. Securing these devices and the data passing between them is a challenging task because the number of IoT Botnet attacks is also increasing sharply year by year. To address this issue, a large number of defenses against network attacks have been proposed in the literature. Despite all the efforts made by researchers in the community over the last two decades, the network security problem is not completely solved. In general, defense against network attacks consists of preparation, detection, and reaction phases. The core element of a good defense system is an IoT Botnet Attack Detection System (IBA-DS), which provides proper attack detection before any reaction. An IBA-DS aims to detect IBAs before they seriously damage the network. The term IBA refers to any unauthorized attempt to access the elements of a network with the aim of making the system unreliable.*

Key words: IoT Botnet, Distributed Denial of Service, Machine Learning, Deep Learning, the Detection system

1. INTRODUCTION

In today's hasty world, one cannot think of life without the internet. Internet is required in different fields like education, business, shopping, communication, etc. Despite many advantages, many evils have been generated over the internet, especially which leads to miscommunication, attacks, hacking, etc. In recent times, the Internet of Things (IoT) is very fast developing with many devices that are convenient in the smart home, smart city, and many other smart systems for education, organization, etc. But there is indeed malware that is targeting the IoT devices. Accordingly, it is necessary to design or develop systems effective for the detection of such types of malwares.

Botnets are generally assembled to affect as many devices as possible and more complex botnets even self-regard and update their behavior, finding and affecting devices accordingly. An IoT botnet is a grid of devices connected to the internet of things (IoT), typically routers, that have been affected by malware and have collapsed under the control of malicious actors.[5] IoT botnets are known for being used in immersing distributed denial-of-service (DDoS) attacks on target entities to disturb their operations and services. Distributed Denial of Service (DDoS) attack is the most common significant threat to online service providers. It involves the attacker's ability to negotiate the availability of web services offered by the targeted host. This is achieved by using attacking agents such as botnet and or compromised Internet of Things (IoT) devices to exhaust the victim's computing capacity (Network Bandwidth, System and Application resources) preventing service availability to legitimate users. There are many techniques that as Machine Learning, Deep Learning, etc., to detect DDoS attacks. Of these techniques, the Deep learning technique is more suitable to detect DDoS attacks.

A detection system continuously checks network traffic and signals any developing attacks in the network. This should then generate a response mechanism that will solicit to assure the network resources and maintain a satisfactory level of quality of service for the genuine users. The success of a detection mechanism is determined by its probability of correct detection, false alarm, and missed detection, and its ability to reach detection decisions quickly in real-time and consume minimal processing resources.[1].

The paper is organized into five sections. The current section is about the challenges of botnet attacks and the detection systems. In section 2 the Literature Survey of the botnet-attack detections researches will be addressed. Furthermore, in section 3 methodology will be presented.

In section 4 the experiment results will be discussed. Decisively, in section 5 the discussion will be concluded.

2. LITERATURE SURVEY

Denial of service(DoS) attacks are immensely easy to dispatch, but the handling of such types of attacks is very difficult. The three generic stages i.e., Detection, Classification, and Response are used to create a system for the detection of DoS attacks. In DoS detection mainly we are analyzing the incoming traffic which is the same as a pattern recognition problem, for this various machine learning techniques have been used. Building effect detection system author used a Bayesian classifier for calculating likelihood ratios of the existence of attacks, which act as a statistical preprocessing method for extracting the features and these features are combinedly used in Recurrent Random Neural Network (r-RNN) for making a comprehensive decision regarding the attack detection. RNNs function the same as the biophysical neural network as it is a biologically influenced framework, where signals are not analog signals. So, this RNN structure we are using for analyzing real-time Statistical data and also differentiates traffic during the DoS attack.[1]

Integrity, Confidentiality, or Availability of any resource is the basic most Important terminologies related to security. Any set of actions that tries to negotiate above mention terms for any resource is Intrusion. The DDoS attack is increasing nowadays because they used packets like the legitimate user. There are different tools that can be used for collecting the features like Trinoo, Synk4, TFN, TFN2k, and Stacheldraht. These tools use the specific port number and protocol, but they can be easily changed so it is difficult to detect DDoS attacks. The proposed system used the data mining approach which uses an automatic feature selection mechanism. The decision tree algorithm is one of the data mining technologies used for the selection of features. Using these features, they build classifiers based on neural networks.[3]

The proposed system involves the analysis of three algorithms Logistic Regression (LR), Support Vector Machine (SVM), and Random Forest (RF).LR is used to model the probability of a certain class. SVM uses a hyperplane that divides the data into two categories. RF algorithm is a classifier that uses multiple trees for making a decision or prediction. For the detection system main focuses is on network traffic. This traffic is summarized as, Originating from this packet's source MAC and IP address and packet's source and destination TCP/UDP Socket. The data pre-processed sung Z-score normalization. The three algorithms or classifiers (LR, SVM, and RF) were used as binary classifiers on normalized data and used in the prediction system. [5]

The proposed system involves the detection of attacks using a Bayesian classifier. The author used different approaches which include the selection of the input features, statistical information gathering, and decision making. For Selecting Input Features, they chose Statistical features like Bitrate, Increase in Bitrate, Entropy, Hurst Parameter, Delay, and Delay Rate. The second is statistical information gathering, it comprises two phases i.e., training probability density function and computations of likelihood. After these two approaches, the victim machine continuously analyzes incoming traffic and based on likelihood probabilities, computational probability is used with a recurrent random neural network (r-RNN)for taking the decision regarding the attack. [2]

The concerns shown and contributions made by the various research groups have therefore attracted the attention of both the industry and academia sectors to come up with a detection technique or mechanism which will serve as the first line of defense against DDoS attacks mitigation. This is because the research groups all support the fact that online services are under attack and therefore need an effective and efficient system to help detect the presence of DDoS attacks on the network infrastructure so that the right mitigation techniques are applied before its devastating effects are experienced by users.

In view of the line of discussion, this research work focuses on using a deep learning technique called Long Short-Term Memory (LSTM) Recurrent Neural Networks (RNN) to develop and train a tensor artificial intelligence (AI) model which will detect the presence of IoT Botnet attack traffic patterns on the network, and achieve a high detection accuracy, and a low false alarm rate.

LSTM RNN was chosen as the technique for this work because, among the family of RNN techniques and existing conventional machine learning techniques, LSTM RNN is rated as the best.

This rating is as result of its ability to learn longer historical features during training time.

Also, unlike the other techniques, LSTM is able to resolve the vanishing gradient problems associated with vanilla RNNs with BPTT by ensuring that a constant error is maintained to allow the RNN to learn over long time steps.

Lastly, LSTM has the ability to use its gated cell state, which makes it act like a computer's memory to make decisions on what data is allowed to be written to it, read from it, and store data on it, to keep features of attacks learned from the training process and make detection decisions based on this stored information on gated cell. Also, the LSTM has been able to achieve an accuracy rate of 97.996% [55] which the older machine learning technique has not been able to achieve.

Tensor Flow was also chosen as the machine learning implementation platform because it has a flexible architecture that supports CPU, GPU, Android, and iOS. This makes it easy to port trained models to any other hardware without any code changes. It is also simple to train its mathematical functions useful for neural networks.

3. METHODOLOGY

The anomaly-based intrusion detection system is a kind of method which works on the fact that malicious activities are different from typical user activities. Intrusion is defined as the difference between abnormal user behavior and standard user behavior. There are two phases in the development of AIDS: the training phase and the testing phase. In the training phase, the normal traffic profile is used to learn a model of normal behavior. In the testing phase, a new data set is used to develop the system's capacity to generalize to previously unseen intrusions.

AIDS method is categorized into four groups: Supervised learning, Unsupervised learning, reinforcement learning, and deep learning. These methods are used to extract the knowledge from datasets using different algorithms and techniques such as clustering, neural networks, association rules, decision trees, genetic algorithms, CNN, RNN, etc., and train the machine based on knowledge.

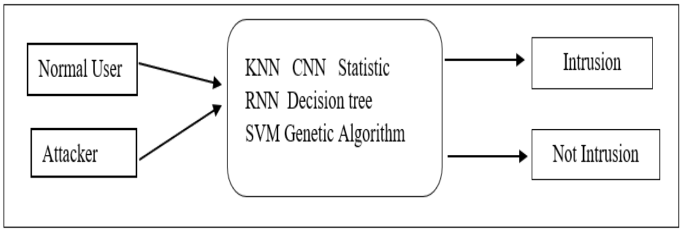

Figure 1. Conceptual Learning based on AIDS

Various signature-based detection methodologies to evolve an efficient model for the detection of attacks. Some detection methods are listed below:

- Statistics based: Complex statistical algorithms are used to analyze the network and process the information.
- Pattern-based: This method identifies different patterns, the characters, and forms in the data
- Rule-based: To detect a potential attack on the suspicious network traffic it uses an attack "signature".
- State-based: State-based method examines a stream of events to identify any possible attack.
- Heuristic-based: It is based on activity.it identifies any abnormal activity that is out of the ordinary activity.

4. EXPERIMENTAL SETUP

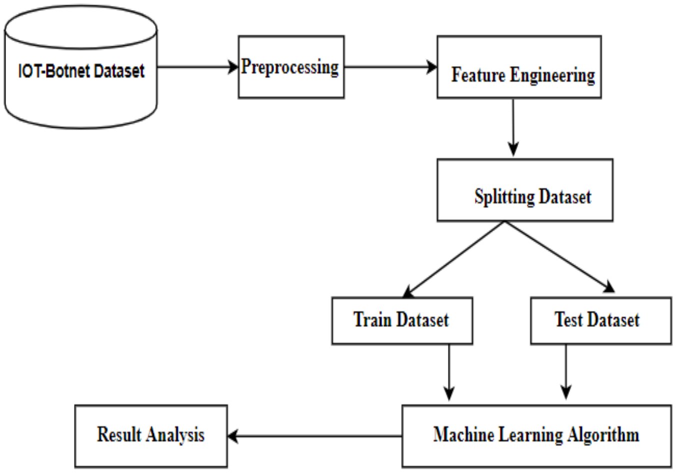

Figure 2. Proposed Experimental Setup

- Data Collection:

  First step is to collect data. We will collect UNSW NB-15 dataset. This dataset has 4 CSV files of data records and each CSV file contains attack and normal records.

- Data Preprocessing:

  In this step, we will clean the data. We will manipulate or drop the data before it is used to ensure or enhance performance.

- Feature Extraction:

  The aim of this step is to reduce the number of features in a dataset by creating new features from the existing ones (and then discarding the original features).

- Splitting Dataset:

  The Dataset is split into Training Dataset and Test Dataset

- Machine Learning Algorithm:

  Using the training dataset train the model with various machine learning methods like Bayesian classifier, support vector machine, neural network, etc.

- Result Analysis:

  Applying the test dataset to the model or the trained system for analyzing the result using various parameters such as Accuracy, Precision, Recall, and F1-score

5. CONCLUSION

In this paper, we have reviewed different approaches for designing the best DDoS attack detection model. We learn different machine learning algorithms and deep learning algorithms like SVM, naïve Bayes, random forest, decision tree, and neural network are used for the development of the system for prediction of attack. We understood the general flow of the prediction system. We analyze the result of different algorithms. To determine the accuracy and efficiency of the algorithm, it was evaluated against seven main parameters such as dataset size, epochs, learning rate, nodes, weights, and biases. There was a lot of iteration done to get the best results. Every iteration done involved assigning different values to parameters such as datasets size and epochs while randomly generated values for weights and biases were used, layers, nodes, and learning rate were held constant until the best detection accuracy was achieved.

REFERENCES

[1] G. Loukas, and O. Gulay. "Likelihood ratios and recurrent random neural networks in the detection of denial-of-service attacks."

[2] G. Oke, G. Loukas and E. Gelenbe, "Detecting Denial of Service Attacks with Bayesian Classifiers and the Random Neural Network," 2007 IEEE International Fuzzy Systems Conference, London, pp. 1-6.

[3] M. Kim, H. Na, K. Chae, H. Bang, and J. Na: A Combined Data Mining Approach for DDoS Attack Detection, Lecture Notes in Computer Science, Vol. 3090, pp. 943-950.

[4] MRUTYUNJAYA PANDA, ABD ALLAH A. MOUSA, AND ABOUL ELLA HASSANIEN, "Developing an Efficient Feature Engineering and Machine Learning Model for Detecting IoT Botnet Cyber Attacks" Received June 14, 2021, accepted June 18, 2021, date of publication June 24, 2021, date of current version July 1, 2021

[5] SIKHA BAGUI, XIAO JIAN WANG, AND SUBHASH BAGUI, "Machine Learning Based Intrusion Detection for IoT Botnet" International Journal of Machine Learning and Computing, Vol. 11, No. 6, November 2021.

[6] MEENAKSHI MITTAL1, KRISHAN KUMAR1, SUNNY BEHAL, "Deep learning approaches for detecting DDoS attacks: a systematic review'' The Author(s), under exclusive license to Springer-Verlag GmbH Germany, part of Springer Nature 2021.