YIDDISH Vol 13 Issue 04, Dce 2023
ISSN NO: 0364-4308

A Two-Fold Machine Learning Method for Identifying and Preventing IoT Botnet Attacks

Dr.T Srikanth[1], K. Mamatha[2], Sushil Kumar[3].

1 Associate Professor & HoD CSE, Malla Reddy Institute Of Technology and Science (UGC- Autonomous),Hyderabad.

2 Assistant Professor , Malla Reddy Institute Of Technology and Science (UGC-Autonomous),Hyderabad.

3 UG Student, Malla Reddy Institute Of Technology and Science (UGC-Autonomous),Hyderabad.

ABSTRACT

The most common cyber-attack in an Internet of Things (IoT) setting, the botnet assault is a multi-stage attack that starts with scanning and concludes with a distributed denial of service (DDoS) attack. The majority of the research being conducted focuses on identifying botnet assaults that occur after hacked IoT devices launch DDoS attacks. Similar to this, the majority of machine learning-based botnet detection algorithms now in use are only as good as the datasets they were trained on. Because of the variety of attack patterns, these solutions do not perform well on different datasets. Therefore, by creating 33 different kinds of scans and 60 different types of DDoS assaults, we first create a generic scanning and DDoS attack dataset in this study. To effectively train the machine learning algorithms, we also partly merged the DDoS attack samples and scan data from three publically accessible datasets for maximum attack coverage. Next, we suggest a dual machine learning strategy to stop and identify Internet of Things botnet assaults. To stop IOT BOTNET assaults, we trained a cutting-edge deep learning model, ResNet-18, in the first fold to identify scanning activity early in the attack phase. In contrast, we trained a second ResNet-18 model for the detection of DDoS assaults in order to identify IoT botnet attacks in the second fold. In order to stop and identify IoT botnet assaults, the suggested two-pronged method exhibits 98.89% accuracy, 99.01% precision, 98.74% recall, and 98.87% f1-score.

1. INTRODUCTION

By allowing actual items and things to connect and interact with one another online to enhance human lives, the Internet of Things (IOT) significantly changed technology [1], [2]. The use of smart IOT devices in our everyday lives has increased dramatically over the last several years, including smart TVs, smart toys, smart wearable's, smart cameras, smart lamps, etc. [3], [4]. As a result, this recent development in the realm of computers has given common items the ability to link and interact with one another without the need for human involvement. IOT devices are useful in many ways, but their security features are either nonexistent or very constrained [3]. Moreover, a set key or hard-coded default username and password are often included with Internet of Things devices, which the user cannot modify [5]. Hackers may easily take control of these unreliable IOT devices by taking advantage of these security flaws [4]. Recent statistics show that as the number of unsecured IOT devices rises quickly, cyber attacks are becoming more frequent [6]. Botnet and distributed denial of service (DDOS) assaults are the most common kind of cyber attacks that have been reported lately. Over the last ten years, these attacks have grown in frequency and severity [4], [6]. A bonnet assault is a kind of cyber attack where the attacker searches a network for Internet of Things (IOT) devices that are susceptible to security breaches. The attacker targets susceptible (IOT) devices and uses malware to implant a bot software into them after analyzing the scanning data [7]. The installed bot program links the compromised devices to a peer network or central server, from which it receives commands to carry out various malicious actions, such as flooding DDOS attacks and sending spam, among other malicious activities, from a large number of compromised IOT devices over the target server, website, etc. An attacker exploits an infected IOT device to launch denial-of-service (DDOS) assaults when the device joins a botnet.

The botnet assault poses a critical risk to the whole internet in addition to being a major hazard to unprotected IOT devices [6]. Since the start of the Mirai botnet assault in 2016, there has been a steady increase in IOT botnet attacks Numerous modifications and clones of the Mirai botnet have emerged since the source code was made available [9]. Over the last several years, these new variations and their imitators have infected millions of IOT devices [3], [9], and unleashed increasingly significant and devastating denial-of-service (DDOS) assaults on sites like GitHub [10], AWS [11], etc. Attackers may now quickly identify unsecured IOT devices by using internet resources like Censys [13], Shodan [12], etc. A wealth of information may be found using these internet search engine services to target unsecure IOT devices [9]. An attacker may carry out a variety of cyber attacks, including spamming, phishing, denial-of-service assaults (DDOS), and more by breaking into unprotected Internet of Things devices. This allows them to cause havoc with other online resources. IOT devices are far more vulnerable to botnet and distributed

denial of service (DDOS) assaults, according to certain recent research [14], [15]. A variety of DDOS attacks are carried out by hacked IOT devices. Similarly, a recent prediction by Gartner indicated that 25% of cyber attacks are caused by unsecured Internet of things devices [16].
There has to be an effective security solution to identify IoT bots in order to prevent vulnerable IOT devices from turning into bots and carrying out various DDOS assaults. There are two types of current bonnet and DDoS attack detection systems: host-based approaches and network-based techniques [17]. Host-based solutions are not practical for IOT devices because of their limited resources (memory, battery life, and computational capacity) [1], [17]. To further defend the network and IOT devices from these severe cyber attacks, a network-based solution is recommended. Three primary categories include the network-based approaches [18]_[22]:
1) Signature-based detection method: uses a set of precise rules stored in a rule database to compare network traffic with in order to identify and stop possible attacks.
2) Anomaly-based detection technique: evaluates typical network traffic patterns and creates a baseline profile of every device connected to the network. Any notable departure from the standard is seen as an oddity. There are two further subtypes of the anomaly-based detection approach. V
_ Statistics-based detection: These techniques use a statistical distribution of incursions to identify abnormalities.
_ Machine learning-based detection technique: uses payload and packet attributes to identify anomalies. These techniques mostly use machine learning models to identify and stop possible threats[7][8].
_ Knowledge-based detection method: identifies abnormalities by examining a network's profile or history. To find anomalies in the network, the profile or prior knowledge of the network is built under various test scenarios [22].

2. LITERATURE SURVEY

A graph-based method for identifying IoT botnets by printing string information (PSI) graphs was presented by Nguyen et al. [16]. The function call graph's high-level properties were extracted by the authors using PSI graphs, and they then trained a convolution neural network (CNN), a deep learning model, using the resulting graphs to identify IoT bonnets. Similar to this, BotMark is an automated model that Wang et al. [24] suggested. Their suggested technique uses a hybrid analysis of flow-based and graph-based network traffic characteristics to identify botnet assaults. K-means, which computes the similarity and stability scores between flows, carries out the flow-based detection. On the other hand, the least squares method and the local outlier factor (LOF), which calculates anomaly scores, are used in the graph-based identification.
Likewise, Yassin et al. [25] presented a revolutionary technique that undermines many strategies, including using the frequency process against registry data, visualizing graphs, and generating rules. The authors used a graph-theoretical technique to study the Mirai assaults. The authors used directed graphs to determine which Mirai patterns were similar and which weren't. The suggested strategy is limited to addressing the Mirai assault.
A hybrid botnet detection approach was presented by Almutairi et al. [27] to identify newly created bonnets that operate on three different levels: host level, network level, or a mixture of both. The writers concentrated on DNS, P2P, IRC, and HTTP botnet activity. Three parts make up the suggested technique: a detection report, a network analyzer, and a host analyzer. For the purpose of classifying traffic, the authors used two machine learning algorithms: a decision tree and Naïve Bayes.
In a similar vein, Blaise et al. [28] suggested BotFP as a bot fingerprinting identification method. The suggested BotFP framework comes in two flavors: BotFP-Clus clusters comparable traffic instances using clustering methods, while BotFP-ML uses two supervised machine learning (ML) algorithms—SVM and MLP—to detect new bots based on signature analysis. Similarly, Soe et al. [30] created a strategy for detecting IoT botnet attacks based on machine learning. The model builder and assault detector are the two processes that make up the suggested model. Step-by-step processes for data gathering, classification, model training, and feature selection are carried out during the model builder stage. The packets are initially decoded in the attack detector stage, and then the features are extracted using the same methodology as in the model builder phase. Ultimately, the characteristics are sent to the attack detector engine, which uses machine learning models from Naïve Bayes, J48 decision trees, and artificial neural networks (ANN) to identify botnet attacks. A deep learning-based approach for detecting IoT botnet attacks was presented by Sriram et al. [31]. The suggested method took into account network traffic flows in particular. These are then transformed into feature records and sent to a deep neural network (DNN) model for the purpose of detecting IoT botnet attacks. By conducting a few trials, Nugraha et al. [32] assessed the effectiveness of four deep learning models for botnet attack detection. According to the trial findings, CNNLSTM performed better at detecting botnet assaults than any other deep learning model.
Disadvantages

An established approach identifies the DDoS assault for both incoming and outgoing traffic, hence preventing botnet attacks by recognizing the scanning attack activity. An IoT botnet attack doesn't start with scanning and finishes with a DDoS assault.

3. PROPOSED SYSTEM

The suggested approach created a generic dataset by creating 33 different kinds of scans and 60 different kinds of DDoS assaults after analyzing the commonly used scanning and DDoS attack strategies. Furthermore, in order to optimize the training of machine learning algorithms, we partly merged the scan and DDoS attack samples from three publicly-available datasets. In the context of an Internet of Things network, the system suggested using two different machine learning techniques to stop and identify incoming and outbound bonnet assaults. The suggested dual strategy identifies the DDoS assault to identify the IoT botnet attack and stops it by detecting scanning activities. Lastly, we trained three ResNet-18 models across three distinct datasets and compared their performance with the suggested two-fold technique for identifying and averting IoT botnet attacks to show that the effectiveness of the suggested two-fold approach is not restricted to a single dataset. The method suggested a unique two-pronged machine learning strategy to identify and stop botnet assaults in Internet of Things networks. The suggested approach halts an attacker in the middle of the scanning process, preventing them from moving on to next attack phases.

4. IMPLEMENTATION

Service Provider
The Service Provider must provide a valid user name and password to log in to this module. Upon successful login, he may do several functions including logging in, browsing, and accessing Train & Test Data Sets. View the results of trained and tested accuracy, view the prediction of botnet detection status, view the ratio of botnet detection status, download predicted data sets, and view the accuracy in a bar chart. View All Remote Users, View Botnet Detection Status Ratio Results.
See and Give Users Permission
The administrator may see a list of all enrolled users in this module. The administrator may see user information here, including name, email address, and address, and they can also approve people.
Remote Operator
There are n numbers of users in this module. Registering is required before doing any operations. The user's information is saved in the database when they register. Following a successful registration, he must use his approved user name and password to log in. After logging in successfully, the user may do various tasks such as VIEW YOUR PROFILE, REGISTER, AND LOGINPREDICT BOTNET DETECTION TYPE.

5. CONCLUSION

In order to stop and identify IOT botnet assaults, we suggested a two-pronged machine learning strategy in this paper. In the first fold, we trained the ResNetScan-1 model—a cutting-edge deep learning model—for scanning assault detection using ResNet-18. In the second fold, we trained an additional ResNet-18 model (called the ResNetDDoS-1 model) to identify DDOS attacks in the event that the scanning detection model is unable to stop a botnet assault. We conducted a few experiments where we took the scan and DDOS traffic samples from three publicly-available datasets, trained the ResNet-18 model over these datasets, and saved the resulting Res Net Scan and Res Net DDOS models in order to authenticate the performance of the proposed ResNetScan-1 model and ResNetDDoS-1 model. Next, we put each of the resulting Res Net Scan and Res Net DDOS models to the test using a different set of untrained datasets. The experimental findings showed that, when tested on datasets they had not been trained on, the performance of all Res Net Scan and Res Net DDOS models—aside from the suggested ResNetScan-1 and ResNetDDoS-1 model—significantly decreased. Moreover, the trial outcomes demonstrated that the suggested ResNetScan-1 and ResNetDDoS-1 models maintained their effectiveness and surpassed all other models in identifying scan and DDOS assaults. As a result, the suggested two-pronged strategy is effective and reliable for stopping and identifying IOT botnet assaults with a wide range of attack patterns.
Of the 60 varieties of DDOS assaults, only 33 types of scanning are covered in the present study. As we develop the suggested framework for more effective IOT botnet and DDOS attack prevention and detection, we want to cover

additional scanning and DDOS attack methodologies in the future. Additionally, we can test the suggested dual strategy's efficacy on actual network traffic by deploying it in an intrusion detection system.

REFERENCES

[1] I. Ali, A. I. A. Ahmed, A. Almogren, M. A. Raza, S. A. Shah, A. Khan, and A. Gani, ``Systematic literature review on IoT-based botnet attack,'' IEEE Access, vol. 8, pp. 212220_212232, 2020.

[2] S. Ghazanfar, F. Hussain, A. U. Rehman, U. U. Fayyaz, F. Shahzad, and G. A. Shah, ``IoT-Flock: An opensource framework for IoT traf_c generation,'' in Proc. Int. Conf. Emerg. Trends Smart Technol. (ICETST), Mar. 2020, pp. 1_6.

[3] M. Safaei Pour, A. Mangino, K. Friday, M. Rathbun, E. Bou-Harb, F. Iqbal, S. Samtani, J. Crichigno, and N. Ghani, ``On data-driven curation, learning, and analysis for inferring evolving Internet-of-Things (IoT) botnets in the wild,'' Comput. Secur., vol. 91, Apr. 2020, Art. no. 101707.

[4] F. Hussain, S. G. Abbas, M. Husnain, U. U. Fayyaz, F. Shahzad, and G. A. Shah, ``IoT DoS and DDoS attack detection using ResNet,'' in Proc. IEEE 23rd Int. Multitopic Conf. (INMIC), Nov. 2020, pp. 1_6.

[5] S. Dange and M. Chatterjee, ``IoT botnet: The largest threat to the Ionetwork,'' in Data Communication and Networks. Singapore: Springer, 2020, pp. 137_157.

[6] F. Hussain, S. G. Abbas, U. U. Fayyaz, G. A. Shah, A. Toqeer, and A. Ali, ``Towards a universal features set for IoT botnet attacks detection,'' in Proc. IEEE 23rd Int. Multitopic Conf. (INMIC), Nov. 2020, pp. 1_6.

[7] Y. Madhusekhar, P. Sandhya Priyanka, Deena Babu Mandru, T. Srikanth "Blockchain: A Safe Way to Transfer Signatures in a Distributed Intrusion Detection System" In book: Intelligent Manufacturing and Energy Sustainability (pp.261-273) June 2023 DOI:10.1007/978-981-19-8497-6_26.

[8] BADDAM NAGARANI1, THURIMELLA SRIKANTH2 "Reliable Data Assurance Among Peer-to-Peer Systems" IJSETR Volume.04, IssueNo.25, July-2015, Pages: 4870-4874.

[9] T.Srikanth , Sateesh Nagavarapu , K.Umapavankumar , Narahari D "Commonly used Algorithms in Data Science Along with Internal Logics and Implementations through R Programming"(IJEAT) ISSN: 2249-8958 (Online), Volume-9 Issue-3, February 2020 DOI: 10.35940/ijeat.C5811.029320.