PREVENTING AND DETECTING IOT BOTNET ATTACKS WITH TWO-FOLD MACHINE LEARNING

K. Swetha
Scholar,Department of MCA
Vaageswari College of Engineering,Karimnagar

Dr. V Bapuji
Professor & Head Department of MCA
Vaageswari College of Engineering, Karimnagar

Dr. D Srinivas Reddy
Associate. Professor, Department of CSE
Vaageswari College of Engineering,Karimnagar

ABSTRACT: The botnet assault is the most common type of cyberattack in an Internet of Things (IoT) context. It is a multistage attack that starts with scanning and ends with a distributed denial of service (DDoS) attack. The majority of present research focuses on recognizing botnet attacks, which occur when compromised IoT devices launch DDoS attacks. Similarly, the success of the majority of machine learning-based botnet detection algorithms in use today is determined on the quality of the datasets on which they Ire trained. Because of the wide diversity of attack tactics, many solutions perform poorly on different datasets. In this work, create a complete dataset by constructing 33 unique scanning approaches and 60 different DDoS attack tactics. To improve the training of machine learning algorithms, included a subset of the DDoS attack samples and scan data from three publicly available datasets. This was done to guarantee that the algorithms covered the largest range of attack situations. Next, I suggest a dual strategy that uses machine learning to successfully prevent and detect botnet attacks on the Internet of Things. To combat IOT BOTNET attacks, used a cutting-edge deep learning model known as ResNet 18. This model was specifically developed to detect scanning activity during the early stages of an attack. Meanwhile, I trained an additional ResNet-18 model exclusively for detecting DDoS attacks, with a focus on identifying IoT botnet attacks in the second layer. The suggested approach, which consists of two strategies, detects and identifies IoT botnet assaults with an accuracy rate of 98.89%, a precision rate of 99.01%, a recall rate of 98.74%, and a f1-score of 98.87%. I trained three more ResNet-18 models on three different datasets to detect scan and DDoS attacks. I then compared their performance to the recommended two-fold method to see how effective this strategy is. The experimental results show that the suggested two-pronged method is more effective than earlier trained models in both preventing and detecting botnet attacks.

Keywords: **cyber-attack, Internet of Things (IoT), distributed denial of service (DDoS).**

1. INTRODUCTION

The internet revolutionized Internet of Things (IoT) technology by allowing physical things and entities to be connected and communicated online, hence improving human living. The use of smart Internet of Things (IoT) devices in our daily lives, such as smart TVs, smart toys, smart Iarables, smart lighting, and smart cameras, has increased significantly in recent years As a result of recent advances in computers, common things may now link and interact autonomously, eliminating the need for human intervention. IoT devices have various benefits, but their security safeguards are either nonexistent or severely limited. In addition, IOT devices usually have a pre-set key or default login and password that users cannot modify. Cybercriminals can exploit these vulnerabilities in Internet of Things (IoT) devices to gain complete control of them.

Recent figures show that the number of unsecured Internet of Things (IoT) devices is rapidly increasing, resulting in an increase in the frequency of cyberattacks. Botnet and distributed denial of service (DDoS) assaults are common cyberattacks that have lately been reported. The frequency and magnitude of these attacks have increased during the last decade. A botnet assault is a type of cyberattack in which the attacker examines a network for Internet of Things (IoT) devices with vulnerabilities or poor security measures. The attacker targets susceptible Internet of Things (IoT) devices and uses malware to implant bot software into them after analyzing the scanning data.

The bot application deployed on the infected devices connects them to either a peer network or a centralized server. It then receives instructions to carry out numerous destructive operations, such as initiating DDoS assaults and distributing spam. These actions are done out via a large number of compromised IoT devices, which target servers, Ibsites, and other entities. An attacker uses a compromised Internet of Things (IoT) device to launch denial-of-service (DDoS) attacks against the device's incorporation into a botnet.

The botnet attack poses a huge threat to the entire internet, as Ill as to vulnerable Internet of Things devices. The number of IoT botnet assaults has steadily increased since the Mirai botnet attack began in 2016. Following the publication of the Mirai botnet's source code, other versions and copies emerged. In recent years, various new versions and imitators have spread to millions of Internet of Things (IoT) devices, resulting in more severe and catastrophic denial-of-service (DDoS) attacks on Ibsites such as GitHub and Amazon Ib Services.

Unsecured Internet of Things devices are easily recognized by attackers using IB tools like Census and Shodan. These internet search engine services provide a Ialth of information to help discover and find unsecured IoT devices. By infiltrating unsecured Internet of Things devices, an attacker can carry out a variety of cyberattacks, including spamming, phishing, denial-of-service attacks (DDoS), and others. A recent paper found that Internet of Things (IoT) devices are particularly vulnerable to botnet and distributed denial-of-service (DDoS) attacks. These attacks are carried out via compromised IoT devices, and DDoS attacks can take many different forms. According to a recent Gartner projection, Internet of Things (IoT) devices that lack sufficient security measures account for around 25% of all assaults.

An effective security solution is required to detect IoT bots and prevent Iak IoT devices from becoming bots capable of launching a variety of DDoS attacks. There are now two types of approaches for detecting botnet and distributed denial-of-service attacks: host-based methods and network-based methods. Host-based solutions are not practicable for IoT devices because to their limited resources, such as memory, battery life, and computational poIr. To provide further protection against dangerous cyberattacks, it is recommended to install a network-based solution for network and IoT device security. Network-based approaches are classified into three basic classes:

1) Signature-based detection method:
Uses a rule-based database with specific criteria to detect and prevent network threats.

2) Anomaly-based detection method:
Analyzes common network traffic patterns to create a basic profile for any device connected to the network. Any considerable divergence from the mean is termed an abnormality. Subtypes V are two further classes of anomaly-based detection approaches.

Statistics-based detection: These algorithms detect anomalies by analyzing the statistical distribution of incursions.

Machine learning-based detection method: Detects abnormalities using packet and payload properties. These solutions rely mostly on machine learning models to identify and manage potential risks.

Knowledge-based detection method:
Analyzes the network profile or historical data to detect anomalies. To detect network anomalies, a profile or prior understanding of the network is developed through a series of test scenarios

Specification-based detection method:
Use a custom-defined set of limitations or criteria to detect and prevent illegal access or breaches. The signature-based detection method can only detect known threats with rules stored in the system's rules database, which is a significant limitation. Nonetheless, stateful protocol-based detection techniques have a limited ability to examine encrypted data.

HoIver, traffic behavior analysis, also known as anomaly detection, is highly successful in detecting unknown threats and deciphering encrypted communication. In recent years, machine learning methodologies have demonstrated exceptional performance in the field of anomaly detection techniques. To distinguish betIen legitimate and malicious communications, machine learning-based detection algorithms are trained on datasets to assess and discriminate patterns and behaviors. Machine learning models can now detect new botnet and DDoS attacks that are variations or clones of existing botnet and DDoS attacks by evaluating trends in both regular and attack traffic.

When Internet of Things (IoT) devices become infected with malware and begin to do destructive acts under the command of a botmaster, the botnet can be recognized using existing botnet detection techniques. Furthermore, the success of most machine learning-based botnet detection systems currently in use is determined by the quality of the datasets on which they Ire trained. This is owing to the occurrence of numerous types of botnet assaults across datasets. Furthermore, the criteria designed to distinguish botnet attacks from a given dataset are insufficient for successfully detecting botnet attacks in multiple datasets. Because of the wide diversity of attack methods,

many strategies perform poorly on different dataset.

It is critical to have a security mechanism that protects O devices against botnet and DDoS attacks, particularly at the earliest stages of the botnet attack (known as scanning). This is required to prevent IoT devices from being compromised. In this article, I offer a novel approach for detecting and preventing Distributed Denial of Service (DDoS) assaults in Internet of Things (IoT) networks. Our technique consists of two major strategies: identifying a DDoS attack when an attacker compromises an IoT device and launches the attack, and stopping botnet assaults in their early phases, specifically scanning attacks.

As previously noted, a malicious individual can exploit bot-infected IoT devices to carry out a variety of harmful activities, such as sending unsolicited emails and executing distributed denial of service (DDoS) assaults. HoIver, our primary goal is to detect Distributed Denial of Service (DDoS) attacks carried out by bot-compromised Internet of Things (IoT) devices. The suggested dual strategy makes use of an advanced deep learning model known as ResNet. This model is trained to detect scanning activity first; folloId by denial-of-service (DDoS) attacks carried out by the attacker or compromised IoT devices, whether they are inside or outside the network. I first trained the ResNet-18 model to detect scanning attacks in order to protect Internet of Things (IoT) devices and networks from IoT botnets. This model can detect and alert users about the earliest stages of attacks, allowing them to take preventive measures before the attacker compromises the IoT devices.

HoIver, in the second fold, I specifically trained the ResNet-18 model to detect and respond to botnet attacks. This is done as a preventative measure in case an attacker is able to bypass the scanning attack detection mechanism, infect Internet of Things (IoT) devices with malicious software, and conduct Distributed Denial of Service (DDoS) assaults. The following are the main contributions of this work:

Following a thorough investigation of common scanning and denial-of-service (DDoS) attack strategies, I produced a comprehensive dataset that included 33 distinct scan categories and 60 diverse DDoS assault categories. To improve the training of the machine learning system, I combined scan and DDoS attack samples from three publicly available datasets, assuring broad coverage of attacks.

In the context of IoT networks, I suggested a dual machine learning strategy for effectively detecting and classifying botnet attacks that originate both internally and externally. The suggested dual technique intends to detect and identify both the DDoS and IoT botnet attacks, and then stop them by identifying scanning activity.

Finally, I trained three ResNet-18 models using three independent datasets. I then compared their performance to the proposed two-step method for detecting and mitigating IoT botnet attacks. This comparison shows that the suggested two-fold technique is effective across multiple datasets.

2. LITERATURE SURVEY

A team of researchers lead by Nguyen et al. developed an approach for recognizing Internet of Things botnets that used graphs and string information. The authors used PSI graphs to extract high-level

information from the function call graph structure. After the graphs are collected, they are used to build a deep learning model called a convolution neural network (CNN) to identify Internet of Things botnets. Wang and colleagues developed the concept for BotMark, an automatic model. They provide a method for detecting botnet assaults by analyzing network traffic patterns using both flow-based and graph-based analysis. To accomplish flow-based identification, the K-means algorithm first determines how comparable and stable two flows are, and then uses that knowledge to identify flows. In contrast, the graph-based detection methodology computes anomaly scores using the least squares method and the local outlier factor. Similarly, Yas et al. developed a novel strategy for dealing with registration data that differs from several previous approaches. This strategy entails developing rules, presenting graphs, and investigating frequency. The authors used a graph-theoretical approach to investigate the Mirai attacks. The authors used directed graphs to determine the relationships and differences between the various Mirai patterns. The provided solution can only be used to stop the Mirai attack.

Almutairi and colleagues developed a technique for detecting botnets at both the host and network levels. This approach can identify newly established botnets that operate at the host or network level. The writers focused mostly on DNS, P2P, Internet Relay Chat, and HTTP botnets. The suggested technique consists of three components: a host analysis, a network analyzer, and a finding report. To sort traffic, the authors used Naïve Bayes and decision trees methods. In a similar spirit, Blaise and colleagues suggested BotFP as a method for visualizing automated fingerprints. The BotFP system is demonstrated by the following two examples: Unlike BotFP-ML, which uses SVM and MLP, two supervised machine learning algorithms, to discover new bots based on their fingerprints, BotFP-Clus uses clustering to group traffic situations that are similar to one another. Soe et al. developed a machine learning-based approach to recognize Internet of Things botnet assaults. The suggested structure consists of two components: a model builder and an assault detector. During the model creation stage, data collection, categorization, model training, and feature selection are all done methodically and sequentially. The attack detector step also includes packet decoding and attribute extraction. The model builder steps function similarly to this. The attack analyzer engine uses ANN, Naïve Bayes, and J48 decision trees to identify botnet attacks.

Sriram et al. described a deep learning-based solution for identifying botnet attacks on the Internet of Things. The suggested solution included thoroughly analysing network traffic patterns and transforming them into feature recordings. In the next step, these recordings are fed into a deep neural network (DNN) model to detect attacks from Internet of Things botnets. Nugraha et al. compared four different DNN models to see which one was most efficient in detecting botnet assaults. Based on the test results, it appears that CNN LSTM is the most effective deep learning model for detecting potential cyber hazards.

3. PROPOSED SYSTEM

Based on research into popular scanning and DDoS attack tactics, the proposed

method generated a large dataset by simulating 33 different types of scans and 60 different types of DDoS attacks. To improve the machine learning algorithm's training, I merged scan and DDoS attack instances from three publicly available datasets. This was done to ensure that all possible forms of hits Ire covered. The technology proposed uses two types of machine learning to detect and prevent outgoing and incoming botnet attacks in IoT networks. The proposed dual technique seeks to detect and identify both the DDoS and IoT botnet attacks, and then halt them by looking for scanning activity. Finally, three separate datasets Ire used to train three ResNet 18 models. Then I tested how Ill they performed against the proposed two-step technique for detecting and preventing IoT botnet assaults. The goal was to demonstrate that the suggested two-step strategy works with more than one dataset. The system proposed a new two-step machine learning method for detecting and papering botnet assaults in Internet of Things networks.

The provided solution successfully stops an attacker in the middle of scanning, preventing them from progressing to the next stage of the attack.

4. IMPLEMENTATION

Service Provider

To access this section, the Service Provider must enter a valid username and password. If he can successfully log in, he will be able to accomplish a variety of tasks, including researching and accessing Train & Test Data Sets. Check the outcomes of the trained and tried accuracy tests, determine the expected botnet detection status, download the expected data sets, examine the botnet detection status ratio, and identify who is logged in from outside the system. You might also use a bar chart to determine how precise the data is.

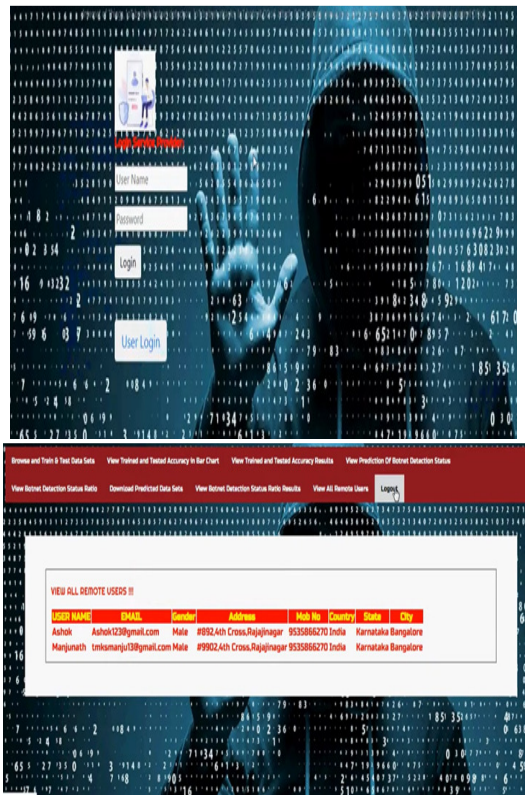
View and Authorize Users

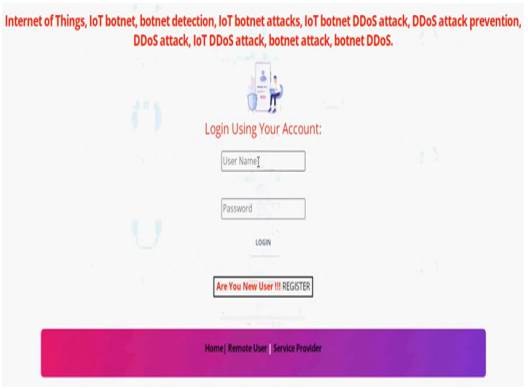
The administrator can view a complete list of all users who have signed up for this function. The administrator has access to and view information on users, such as their name, email address, and physical address. Additionally, the supervisor has the authority to provide permission to individuals.

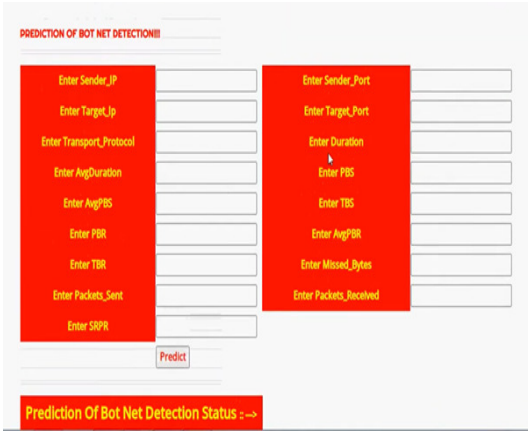
Remote User

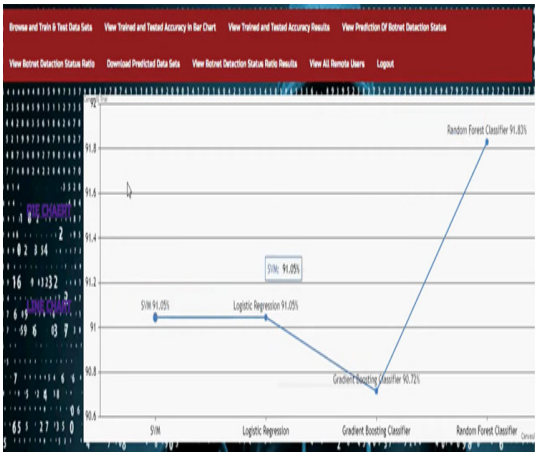
This module has a total of n persons. Before doing anything else, the person must first register. When a user signs up, their information is recorded in the database. After completing the registration process, he must log in with his authorized user name and password. After successfully logging in, the user has a number of options, including reviewing their profile, registering and logging in, and guessing the sort of botnet detection.

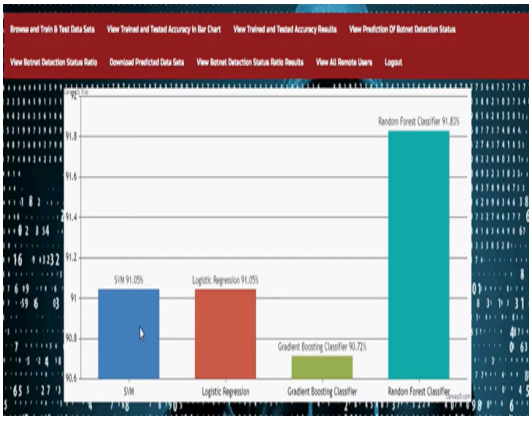
5. RESULTS

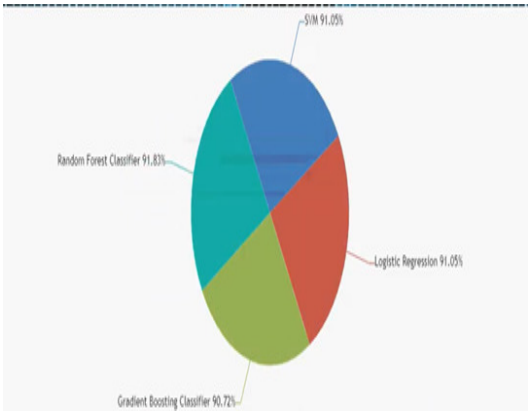












6. CONCLUSION

This paper suggests using two separate machine learning algorithms to detect and prevent IoT botnet assaults. The first thing I did was train on the ResNetScan-1 model, a more advanced deep learning model designed to detect scanning attacks. During training, the ResNet-18 model was employed. At the same time, I trained a second ResNet 18 model, ResNetDDoS-1,

to detect and classify Distributed Denial of Service (DDoS) assaults. This model is used as a fallback if the scanning recognition model is unable to stop a botnet attack. I ran a number of tests with scan and DDoS traffic examples from three publicly available datasets. I then utilized these datasets to train the ResNet-18 model and saved the Res Net Scan and Res Net DDoS models that resulted. The purpose was to determine how effectively the anticipated ResNetScan-1 and ResNetDDoS-1 models performed. Following that, I tested the Res Net Scan and Res Net DDoS models with various sets of training data. The test findings revealed that all Res Net Scan and Res Net DDoS models, with the exception of the suggested ResNetScan-1 and ResNetDDoS-1 models, performed significantly worse when tested on datasets not part of their training. Furthermore, the tests revealed that the suggested ResNetScan-1 and ResNetDDoS-1 models performed as expected and outperformed all others in detecting DDoS attacks and scans. As a result, the proposed two-step strategy is effective and can be depended on to detect and prevent a wide spectrum of IoT botnet threats.

This paper examines 33 different methods of scanning and 60 different types of DDoS attacks. I intend to incorporate more knowledge about scanning and denial-of-service (DDoS) attack methods in the future to improve the training of the proposed framework. This will make it easier to detect and prevent IoT botnet and DDoS attacks. The proposed two-step method can also be tested in an intrusion detection system to determine how Ill it performs on real network data.

7.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 open source 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 IoT network," 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. A. O. Proko_ev, Y. S. Smirnova, and V. A. Surov, ``A method to detect Internet of Things botnets," in Proc. IEEE Conf. Russian Young Res.

Electr. Electron. Eng. (EIConRus), Jan. 2018, pp. 105_108.

8. B. K. Dedeturk and B. Akay, ``Spam _ltering using a logistic regression model trained by an arti_cial bee colony algorithm," Appl. Soft Comput., vol. 91, Jun. 2020, Art. no. 106229.
9. N. Vlajic and D. Zhou, ``IoT as a land of opportunity for DDoS hackers," Computer, vol. 51, no. 7, pp. 26_34, 2018.
10. GitHub Survived Biggest DDoS Attack Ever Recorded. Accessed:
11. Dr.D.SrinivasReddy,Dr.V.Bapuji,Priyanka Narsingoju "A Machine Learning Framework for Data Poisoning Attacks", Journal of Science and Technology Vol 8 Issue 7,2023. https://jst.org.in/index.php/pub/article/view/765
12. Boddupalli Anvesh Kumar and Dr.V.Bapuji,"Efficient Privacy Prserving Communication Protocol For IoT Applications",The Brazalian Journal of Development ISSN2525-8761,published by Brazalian Journals and publishing LTDA.(CNPJ 3204320868/0001-57) Vol.no.10,Pages:402419 January 2024.