Reducing DDoS Attacks in IOT Networks for Anomaly Detection

K.Nishitha[1], Dr.M.Ussenaiah[2], G.Rajesh[3]
Assistant professor[1], Associate Professor[23], Department of CSE[13], MCA[2],
Audisankara College of Engineering and Technology[13], V S University[2]
Gudur[13], Andhra Pradesh, India

Abstract: The recent surge in the number of Internet of Things (IoT) devices is setting the stage for the rise of intelligent cities, where trillions of IoT gadgets are linked together to offer innovative, widespread services and streamline our everyday activities. However, as the quantity of vulnerable IoT devices is increasing at an alarming pace, the effect of Distributed Denial-of-Service (DDoS) attacks is escalating as well. With the introduction of IoT botnets like Mirai, the perception of IoT has shifted from a facilitator of smart cities to a potent tool for cyber-attacks. This situation calls for the creation of new methods to enhance the adaptability and effectiveness of decision-making in the context of software-defined networks (SDN). Emerging technologies, such as SDN and blockchain, open up fresh possibilities for secure, cost-effective, flexible, and efficient collaboration in DDoS attacks within the IoT space. In this study, we introduce Co-IoT, a blockchain-based system designed for collaborative DDoS attack defense; it employs smart contracts to enable attack collaboration across SDN-based entities and securely and efficiently share attack data. The Co-IoT system is put into practice on the Ethereum official test network Ropsten. The experimental findings demonstrate that Co-IoT delivers flexibility, efficiency, security, and cost-effectiveness, making it a promising approach for mitigating DDoS attacks on a large scale.

Keywords: Internet of Things, Black Chain, Cyber attacks, Denial of Service, Service Oriented Architecture (SOA)

I. INTRODUCTION

In the fast-changing landscape of automated and interconnected gadgets, the entire planet can be seen as a vast network of devices that communicate and connect with each other. The Internet of Things (IoT) represents a pervasive computing environment where sensors and actuators are linked with both living and non-living entities, forming part of the Internet; not just computers and smartphones. However, as this network expands, so do the challenges it faces. IoT security issues carry significant consequences for the domain's future, highlighting concerns regarding the safety of devices in operation. At the same time, distributed denial of service (DDoS) attacks have already affected cyber security. With the Internet of Things, DDoS attacks have surged due to the increased number of devices available for exploitation. The deployment of devices with limited resources in the IoT context has further facilitated the exploitation by attackers. This situation has sparked a surge in research interest in the area of IoT security. Vipindev Adat and B. B. Gupta, both professors at the National Institute of Technology in Kurukshetra, Haryana, are among those leading this research. The IoT ecosystem consists of various devices, each with different attributes and capabilities. Due to the IoT's extensive growth and swift advancement, these devices are becoming more prevalent in smart homes and smart cities. IoT is also described as a network of physical objects or things, equipped with limited computational power, storage, and communication capabilities, all integrated with electronics (such as sensors and actuators).

Mitigating DDOS Attack In IOT Network Environment network connectivity, allowing these objects to gather, process, and exchange data. The objects in IoT are objects from our daily lives, ranging from smart household devices such as a smart bulb, smart adapter, smart meter, smart refrigerator, smart oven, AC, temperature sensor, smoke detector, IP camera, to more sophisticated devices such as frequency Identification (RFID) devices, heartbeat detectors, accelerometers, sensors in the parking zone, and a parking zone sensor. As the use of IoT devices grows, so are the number of abnormalities caused by these devices. To address security challenges such as interruptions, spoofing attacks, Dos attacks, jamming, eavesdropping, spam, and malware, IoT applications must offer information protection. The greatest caution should be exercised

with web-based devices, as the vast majority of IoT devices are web-dependent.

Existing Research gaps are for mitigating Distributed Denial of Service (DDoS) attacks in an Internet of Things (IoT) network environment involve a combination of techniques and technologies. Here are some commonly used approaches.
1. Traffic Filtering and Rate Limiting Network devices such as firewalls and routers can be configured to filter and block traffic that matches known DDoS attack patterns or originates from suspicious sources. Rate limiting can also be applied to restrict the amount of traffic that can be sent from a particular source, preventing the network from being overwhelmed.

2. Anomaly Detection Anomaly detection systems analyze network traffic patterns and behavior to identify deviations from normal activity. By using machine learning or statistical techniques, these systems can detect.

3 Mitigating DDOS Attack In IOT Network Environment and flag traffic that exhibits abnormal characteristics associated with DDoS attacks. Once identified, appropriate actions can be taken to mitigate the attack.

4. Black Hole Routing In this approach, traffic destined for the target IoT devices or services is redirected to a "black hole" or null route. This effectively drops all incoming traffic, including DDoS attack traffic, before it reaches the target. Black hole routing can be implemented at the network edge or through collaboration with internet service providers (ISPs) to divert traffic away from the target network.

5. Traffic Scrubbing and Cleaning Centers Traffic scrubbing involves routing incoming traffic through specialized scrubbing centers that analyze and filter out malicious traffic. These centers use various techniques such as deep packet inspection, traffic profiling, and behavioral analysis to distinguish legitimate traffic from attack traffic. Clean traffic is then forwarded to the target network, while malicious traffic is discarded.

Major drawback in the existing work, the system is less effective due to lack of DDOS Detection in IoT using Machine Learning framework. This system is less performance in which it is clear that Supervised machine learning techniques is absence.

In proposed work, mitigating Distributed Denial of Service (DDoS) attacks in an Internet of Things (IoT) network environment may include the following components and strategies

1. Traffic Analysis and Anomaly Detection Implement an advanced traffic analysis system that monitors network traffic in real-time. This system should use machine learning algorithms and behavior analysis techniques to establish a baseline of normal IoT device communication patterns. Any deviations from the baseline that indicate a potential DDoS attack can be detected and flagged for further investigation.

2. Behavioral Profiling Develop behavioral profiles for each IoT device in the network based on its normal communication patterns. These profiles can include information such as the types of traffic generated, expected traffic volume, and communication protocols used. Deviations from these profiles can be identified as suspicious and subjected to additional scrutiny.

The above research existing gaps can be fulfilled as follows:
1. A novel detection and mitigation technique for stealthy DDoS attacks is proposed, and its time and space complexity is analyze.
2. The proposed scheme of DDOS detection is validated using five different machine learning models. An algorithm is proposed to compute the spamcity score of each model which is then used for detection and intelligent decision making.
3. Based upon the score computed in previous step, the reliability of IoT devices is analyzed using different evaluation metrics.

II. RELATED WORK

The DDoS attack prevention in IoT scenario is relatively less addressed compared to other security issues in IoT environment. But recently more occasions of DDoS attacks in IoT environment have happened and this has attracted research interest from all over the world. In this section, we are analyzing the relevant works to defend DDoS attacks in IoT environment. P. Kasinathan have proposed a solution to UDP (User Datagram Procol)flood attack in an IoT environment using 6LoWPAN. They have

implemented their solution using Ebbits network manager and Suricata for creating a network-based IDS. The proposed scheme had multiple intrusion detection probes in the network to detect the attacks. The DoS protection manager integrated to Ebbits was responsible for detecting attacks from the intrusion alerts. Later, they have enhanced the Intrusion Detection System (IDS) using a security incident and event management system called Prelude and a penetration testing tool named Scapy The IDS was simulated in Contiki OS and produced promising results. However, it has high overheads and complex architectures and components which do not suit the IoT environment. Further, the solution confronts only the UDP flood attack and enhancement has to be done to defend more denial of service attacks. A learning automata based solution to DDoS attacks in IoT networks was proposed by Sudip Misra. They have considered a Service Oriented Architecture (SOA) of IoT network to model their solution. A cross network layered IoT network is implemented in which Learning Automata (LA) concepts are used to automatically choose the best action among the possible actions using learning procedure. The solution was proposed in a layered model with LA system model for DDoS attack detection and alert. This approach has been simulated with variable server capacities and showing positive results. Another recent work was done based on the software defined network model of IoT. They have incorporated three Open Flow management tools. Their security mechanism was developed for DDoS attack detection using anomaly detection. They have used Snort for the rule creation and updating. H.C. Lin 6 SRS Mitigating DDOS Attack In IOT Network Environment and P. Wang have tested their proposed model against ICMP flood attack. However, the proposed scheme is good for mobile devices with decent computational and power capabilities and not preferable for end level IoT devices with low power and computational requirements. Further, the scheme is tested in a specific simulation environment and the real-time update of rules and implementation is yet to be performed.

III PROPOSED WORK

The proposed contribution works is as follows:

1. User The user Authentication is one of the key concern areas that form the part of secured access to data. Iris authentication and recognition approach that Mitigating DDOS Attack In IOT Network Environment helps in authenticating the intended user utilizing the characteristic features of the iris. It is useful to know the user is the real person or someone else impersonating the intended person. User Functionalities 1) Upload Iris Dataset 2) Image Preprocessing 3) Iris Segmentation & Features Extraction 4) Train ANN Algorithm 5) Iris Classification from Test Image 1) Upload Iris Dataset Using this module we will upload dataset images to application. 2) Image Preprocessing Using this module we will resize images to equal size and then normalize pixel values. 3) Iris Segmentation & Features Extraction Using this module we will apply Daugman algorithm to extract iris region and then extract features or pixel values from that IRIS region. 4) Train ANN Algorithm Using this module we will feed extracted features to ANN algorithm to build iris classification or recognition module. 5) Iris Classification from Test Image Using this module we will upload eye image and then Daugman will extract IRIS region and then ANN model will recognized/predict person. 2. System Mitigating Distributed Denial of Service (DDoS) attacks in an IoT network environment requires a comprehensive approach that involves 8 SRS Mitigating DDOS Attack In IOT Network Environment securing both the individual devices. The system stores the dataset given by the user. 1. Device Hardening Ensure that each IoT device module has the latest firmware and software updates to patch known vulnerabilities. Disable unnecessary services and ports to reduce attack surface. 2. Network Segmentation Divide the IoT network into segments based on functionality, device type, or criticality. ImplementVLANs (Virtual LANs) or other network segmentation techniques to limit the lateral movement of attacks. 3. Dataset Mitigating Distributed Denial of Service (DDoS) attacks in an IoT network environment using datasets involves leveraging data-driven approaches to identify and respond to attacks. Mitigating Distributed Denial of Service (DDoS) attacks in an IoT network environment using datasets involves leveraging data-driven approaches to identify and respond to attacks. Here's how you can utilize datasets to enhance DDoS mitigation in an IoT network with modular systems. 1. Data Collection: Collect network traffic data from various IoT modules and devices. This data can include traffic patterns, packet sizes, source and destination IPs, and protocol information. Gather information about device behavior and resource usage under normal operating conditions. 2. Anomaly Detection : Use machine learning algorithms to analyze historical data and identify patterns of normal behavior for each

module. Train models to detect deviations from these patterns, which could indicate potential DDoS attacks.

IV PROPOSED ALGORITHMS

1. NAÏVE BAYES ALGORITHM

Naive Bayes algorithm is a supervised learning algorithm, which is based on Bayes theorem and used for solving classification problems. • It is mainly used in text classification that includes a highdimensional training dataset. • Naïve Bayes Classifier is one of the simple and most effective Classification algorithms which helps in building the fast machine learning models that can make quick predictions. • It is a probabilistic classifier, which means it predicts on the basis of the probability of an object. Some popular examples of Naive Bayes Algorithm are spam filtration, Sentimental analysis, and classifying articles.

Algorithm

Step 1: Calculate the prior probability for given class labels.

Step 2: Find Likelihood probability with each attribute for each class.

Step 3: Put these value in Bayes Formula and calculate posterior probability.

Step 4: See which class has a higher probability, given the input belongs to the higher probability class.

2. RANDOM FOREST ALGORITHM

Random Forest is a popular machine learning algorithm that belongs to the supervised learning technique. It can be used for both Classification and Regression problems in ML. It is based on the concept of ensemble learning, which is a process of combining multiple classifiers to solve a complex problem and to improve the performance of the model. As the name suggests, "Random Forest is a classifier that contains a number of decision trees on various subsets of the given dataset and takes the average to improve the predictive accuracy of that dataset." Instead of relying on one decision tree, the random forest takes the prediction from each tree and based on the majority votes of predictions, and it predicts the final output.

Algorithm

Step 1: Select random samples from a given data or training set.

Step 2: This algorithm will construct a decision tree for every training data.

Step 3: Voting will take place by averaging the decision tree.

Step 4: Finally, select the most voted prediction result as the final prediction result

3. SVM ALGORITHM

Support Vector Machine or SVM is one of the most popular Supervised Learning algorithms, which is used for Classification as well as Regression problems. However, primarily, it is used for Classification problems in Machine Learning. The goal of the SVM algorithm is to create the best line or decision boundary that can segregate n-dimensional space into classes so that we can easily put the new data point in the correct category in the future. This best decision boundary is called a hyperplane. SVM chooses the extreme points/vectors that help in creating the hyperplane. These extreme cases are called as support vectors, and hence algorithm is termed as Support Vector Machine.

Algorithm

Step 1: Load the important libraries >> import pandas as pd >> import numpy as np >> import sklearn >> from sklearn import svm >> from sklearn.model_selection import train_test_split >> from sklearn import metrics.

Step 2: Import dataset and extract the X variables and Y separately,df = pd.read_csv(“mydataset.csv”) = df.loc[:,[„Var_X1“,“Var_X2“,“Var_X3“,“Var_X4“]] >> Y = df[[„Var_Y“]]

Step 3: Divide the dataset into train and test >> X_train, X_test, y_train, y_test = train_test_split(X, Y,test_size =0.3,random_state=123)

Step 4: Initializing the SVM classifier model >> svm_clf = svm.SVC(kernel = „linear“)

Step 5: Fitting the SVM classifier model >> svm_clf.fit(X_train, y_train)

Step 6: Coming up with predictions >> y_pred_test = svm_clf.predict(X_test)

Step 7: Evaluating model’s performance >> metrics.accuracy(y_test, y_pred_test) >> metrics.precision(y_test, y_pred_test) >> metrics.recall(y_test, y_pred_test)

Similarly,an SVM classifier can be created in R also XGBoost • XGBoost is an optimized distributed gradient boosting library designed for efficient and scalable training of machine learning models. It is an ensemble learning method that combines the predictions of multiple weak models to produce a

stronger prediction. XGBoost stands for "Extreme Gradient Boosting" and it has become one of the most popular and widely used machine learning algorithms due to its ability to handle large datasets and its ability to achieve state-of-the-art performance in many machine learning tasks such as classification and regression. • One of the key features of XGBoost is its efficient handling of missing values, which allows it to handle real-world data with missing values without requiring significant pre-processing. Additionally, XGBoost has built-in support for parallel processing, making it possible to train models on large datasets in a reasonable amount of time. XGBoost can be used in a variety of applications, including Kaggle competitions, recommendation systems, and click-through rate prediction, among others. It is also highly customizable and allows for fine-tuning of various model parameters to optimize performance. ADABOOST • There are many machine learning algorithms to choose from for your problem statements. One of these algorithms for predictive modeling is called AdaBoost. AdaBoost, also called Adaptive Boosting, is a technique in Machine Learning used as an Ensemble Method. The most common estimator used with AdaBoost is decision trees with one level which means Decision trees with only 1 split. These trees are also called Decision Stumps. KNN • K-Nearest Neighbour is one of the simplest Machine Learning algorithms based on Supervised Learning technique. • K-NN algorithm assumes the similarity between the new case/data and available cases and put the new case into the category that is most similar to the available categories. • K-NN algorithm stores all the available data and classifies a new data point based on the similarity. This means when new data appears then it can be easily classified into a well suite category by using K- NN algorithm. • K-NN algorithm can be used for Regression as well as for Classification but mostly it is used for the Classification problems. K-NN is a non-parametric algorithm, which means it does not make any assumption on underlying data.

Proposed KNNAlgorithm
Step 1: Importing Libraries. In the below, we will see Importing the libraries that we need to run KNN.
Step 2: Importing Dataset. Here, we will see the dataset being imported.
Step 3: Split Dataset.
Step 4: Training Model.
Step 5: Running Predictions.
Step 6: Check Validation.

V CONCLUSION

In conclusion, it appears that the algorithm in question is relatively straightforward when compared to other existing algorithms, and we have observed enhancements in its performance in this area. The earlier research conducted by Kashinathan introduced complexity into the system with advanced intrusion detection systems and related software components. By integrating our algorithm with the current border router, we are expected to see improvements in response time and other relevant metrics. Moreover, our algorithm outperforms in terms of response time delay and packet delivery rate, as previously noted. The strategy for handling sophisticated attacks through risk transfer represents a fresh approach to mitigating DDoS attacks within the IoT space. Although a similar method has been employed by major corporations and research institutions, the application of risk transfer in IoT has remained unexplored, and we have made progress in this direction. Looking ahead, the dynamic nature of IoT network security, particularly in addressing DDoS attacks, is a critical area of focus. As the IoT ecosystem expands, the need for strong defense strategies becomes more pronounced. Future plans may involve the integration of advanced technologies and strategic approaches. The adoption of security-by-design principles will ensure that security features are incorporated into IoT devices, reducing vulnerabilities. Additionally, network segmentation will be improved with more precise access controls, dividing devices into distinct zones to prevent unauthorized access.

VI REFERENCES

[1] Ashton K, "That Internet of Things thing", RFiD Journal, 2009.
[2] Montenegro G, Kushalnagar N, Hui J, Culler D. "Transmission of IPv6 packets over IEEE 802.15. 4 networks." 2007.
[3] Gubbi J., Buyya R., Marusic S., Palaniswami M., "Internet of Things (IoT): A vision, architectural elements, and future directions", in Future Generation Computer Systems, 29(7), pages(1645-1660), 2013.
[4] Tan L. and Wang N., "Future Internet: The Internet of Things", in 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), 2010.

[5] Mulligan G., “The 6LoWPAN architecture.” Proceedings of the 4th workshop on Embedded networked sensors. ACM, 2007.

[6] Kaoru Hayashi, "IoT Worm Used to Mine Cryptocurrency", Available: http://www.symantec.com/connect/blogs/iot-wormused-mine- cryptocurrency (Last accessed March 2017). BIBLIOGRAPHY Mitigating DDOS Attack In IOT Network Environment .

[7] CVE-MITRE, “Common Vulnerabilities and Exposures”, Available: https://cve.mitre.org (Last accessed March 2017).

[8] Symantec, “Internet Security Threat Report”, Volume 21, April 2016.

[9] Bing M, “The Lizard Brain of Lizard Stresser” Arbor Networks, Available: https://www.arbornetworks.com/blog/asert/lizard- brainlizardstresser/ (Last accessed on March 2017).

[10] Kasinathan P, et al. "Denial-of-Service detection in 6LoWPAN based Internet of Things." 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). IEEE, 2013.