DETECTION AND COMPARITION ANALYSIS OF RANSOMWARE

[1]Ms.E.Padma, [2]Pillutla Sree Mahi, [3]Revuru Tejaswini
[1]Assistant Professor,[2]Graduate Students,[3] Graduate students
Dept. of Computer Science Engineering,
SCSVMV University, Enathur, India

Abstract: The architecture employed in the construction and design of the network's hardware. The network's settings can be modified dynamically. A permanent link prevents network design from changing dynamically in any other way. The application of machine learning algorithms for DDOS attack avoidance. The attack, which uses several coordinated systems to simultaneously target a certain server. The infrastructure layer devices in the SDN control layer are those that connect to the application and infrastructure layers and are managed by this software. Here, a decision tree approach is used in machine learning to identify malicious communications. The decision tree algorithm will produce accurate results.

***Keywords*:** Attacks, DDoS, Decision Tree, Ransomware.

I. INTRODUCTION

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt a server or network's normal traffic by flooding the target or its surrounding infrastructure with a flood of Internet traffic. DDoS assaults involve a number of compromised computer systems as sources of attack traffic to be effective. It is possible to use computers and other networked devices, including IoT gadgets, as machinery. A DDoS attack could be compared to unanticipated traffic jams that block the road from a distance and keep regular traffic from getting to its destination... DDoS assaults are carried out on networks of devices linked to the Internet. These networks are made up of computers and other devices that have malware on them, making it possible for an attacker to control them remotely. (including IoT devices). Once a botnet has been created, an attacker can control an attack by giving each bot remote commands.. This could overload the server or network and result in a denial of service to regular traffic. Separating attack traffic from regular traffic can be challenging because each bot is a valid Internet device. A site or service suddenly becoming slow or unavailable is the most obvious sign of a DDoS attack. Further investigation is typically necessary, though, as a number of factors, such as a real increase in traffic, can cause performance issues that are similar. You can identify some of these DDoS attack telltale signs using traffic analytics tools, suspiciously

high traffic volumes coming from a single IP address or IP range, a deluge of users with the same device, location, or web browser version as you, an unexplained spike in requests for a single page or endpoint, etc. Unusual traffic patterns, such as spikes at strange times of day or patterns that seem out of the ordinaryDepending on the sort of attack, there are additional, more precise indications of a DDoS attack. Defined By separating the control from the data plane devices, networking is a new paradigm that gets beyond the drawbacks of traditional network architecture. Data, control, and application planes are its three different planes. Depending on the controller's choice, the data plane carries the network traffic. By computing the routing tables,

the control plane determines the direction of traffic flow. Other applications, including as load balancers, firewalls, Quality of Service (QoS) apps, etc., are managed by the application plane. By decoupling, SDN architecture enhances network performance.

II. LITERATURE SURVEY

Dong, S., & Sarem, M. (2019). DDoS Attack Detection Method Based on Improved KNN With the Degree of DDoS Attack in Software-Defined Networks. IEEE Access, 8, 5039-5048:The Distributed Denial of Service (DDoS) attack has seriously impaired network availability for decades, and still, there is no effective defense mechanism against it. However, the emerging Software provides a new way to reconsider the defense against DDoS attacks. In this paper, we propose two methods to detect the DDoS attack in SDN. One method adopts the degree of DDoS attack to identify the DDoS attack. The other method uses the improved K-Nearest Neighbors (KNN) algorithm based on Machine Learning (ML) to discover the DDoS attack. The results of the theoretical analysis and the experimental results on datasets show that our proposed methods can better detect the DDoS attack compared with other methods.

Summary**:** Dong, S., & Sarem, M describes the results of the theoretical analysis and the experimental results on datasets to show that our proposed methods can better detect DDoS attack compared with other methods.

Dong, S., Abbas, K., & Jain, R. (2019). A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments. IEEE Access, 7, 80813- 80828: Recently, software-defined networks (SDNs) and cloud computing have been widely adopted by researchers and the industry. However, the widespread acceptance of these novel networking paradigms has been hampered by security threats. Advances in processing technologies have helped attackers in increasing the attacks too, for instance, the development of Denial of Service (DoS) attacks to distributed DoS (DDoS) attacks which are seldom identified by conventional firewalls. In this paper, we present the state of the art of DDoS attacks in SDN and cloud computing scenarios. We especially, focus on the analysis of SDN and cloud computing architecture. Besides, we also overview the research works and open problems in identifying and tackling DDoS attacks.

Summary: Dong, S and the team performed research work and opened problems in identifying and tackling the DDoS attacks.

G u, Y., Li, K., Guo, Z., & Wang, Y. (2019). Semi-supervised K-means DDoS detection method using a hybrid feature selection algorithm. IEEE Access, 7, 64351- 64365:Distributed denial of service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. Therefore, it is necessary to propose an effective method to detect DDoS attack from massive data traffics. However, the existing schemes have some limitations, including that supervised learning methods, need large numbers of labeled data and unsupervised learning algorithms have relatively low detection rates and high false positive rates. To tackle these issues, this paper presents a semi-supervised weighted k-means detection method. Specifically, we first present a Hadoop-based hybrid feature selection algorithm to find the most effective feature sets and propose an improved density-based initial cluster centers selection algorithm to solve the problem of outliers and local optimal. Then, we provide the Semi-supervised K-means algorithm using hybrid feature selection (SKM-HFS) to detect attacks. Finally, we exploit the DARPA DDoS dataset, CAIDA “DDoS attack 2007” dataset, CICIDS “DDoS attack 2017” dataset, and real-world dataset to carry out the verification experiment. The experiment results have demonstrated that the proposed method outperforms the benchmark in the respect of detection performance and technique for order preference by similarity to an ideal solution (TOPSIS) evaluation factor.

Meti, N., Narayan, D. G., & Baligar, V. P. (2017, September). Detection of distributed denial of service attacks using machine learning algorithms in software-defined networks. In 2017 international conference on Advances in computing, communications and informatics (ICACCI) (pp. 1366-1371). IEEE:Software Defined Networking (SDN) is a new promising

networking concept which has a centralized control over the network and separates the data and control planes. This new approach provides abstraction of lower-level functionality and allows the network administrators to initialize, control, change, and manage network behavior programmatically. The centralized control, being the major advantage of SDN can sometimes also be a major security threat. If the intruder succeeds in attacking the central controller, he would get access to the entire system. The controller is highly vulnerable to Distributed Denial of Service (DDoS) attacks which lead to exhaustion of the system resources and cause non-availability of the services given by the controller. It is critical to detect the attacks in the controller at an earlier stage. Many algorithms and techniques have been discovered for this purpose. But less work has been done in the field of SDN networks. Using machine learning algorithms for classifying the connections into legitimate and illegitimate is one such solution. We use two machine learning algorithms namely, the Support Vector Machine (SVM) classifier and the Neural Network (NN) classifier to detect the suspicious and harmful connections.

III. PROPOSED METHODOLOGY

A. EXISTING SYSTEM

Machine learning is becoming more and more prevalent, with classical and machine learning approaches used in computer science. This section discusses the research on DDoS assaults and why machine learning techniques are superior to older ones. The project's current methodology follows a specific path, and a limited number of methodologies are employed for model development. However, the outcome is inaccurate and a lot of memory is needed.The system's drawbacks include the following:Low precision, high complexity, high inefficiency, and skilled personnel.

B. MOTIVATION AND PROBLEM STATEMENT

The virus known as DDOS and RANSOMWARE is used to check for attacks on data to see if they have occurred. However, these attacks can be dynamic and online, making the results inaccurate.

C. PROPOSED SYSTEM

The application that can be considered a useful system since it helps to reduce the limitations obtained from traditional and other existing methods. The objective of this study to develop fast and reliable method which detects the DDoS effects accurately. To design this system is we used a powerful algorithm in a based Python environment. The following advantages of the system are:High efficiency, time saving ,in expensive.

D. MODULES

1) System

CREATE DATASET

The dataset containing text which has to be tested wheather there is any malware present in the data. This data must be in the text or pdf format only no images or vedios are allowed to check.

PRE-PROCESSING

The data collected are intrested Resizing and reshaping the data into appropriate format to train our model. Numpy is used to represent the data. At last we label the data out of which 80% will be used to train the model and 20% is used to test the model.

TRAINING

The pre-processed training dataset is used to train our model using Deep learning and Decision tree.

2) User

Login/Registration

The user can register and login with the credentials to the system. The System allows registered users to get in, SQL is used to store and maintain the data of the registrations.

UPLOAD the data

In this module the user can only upload the data that need to be predicted only if the user has logged into the System. If not, a pop up will shown on the screen saying that the user must login first into the system to upload an image after logging into the system the user will be able to upload an image.

CLASSIFIER MODULE

This is the phase where the data is inserted into the page so that the data can be tested and trained here 20% data is tested and 80%is trained after that data is safe or not safe.

E. PROPOSED ARCHITECTURE

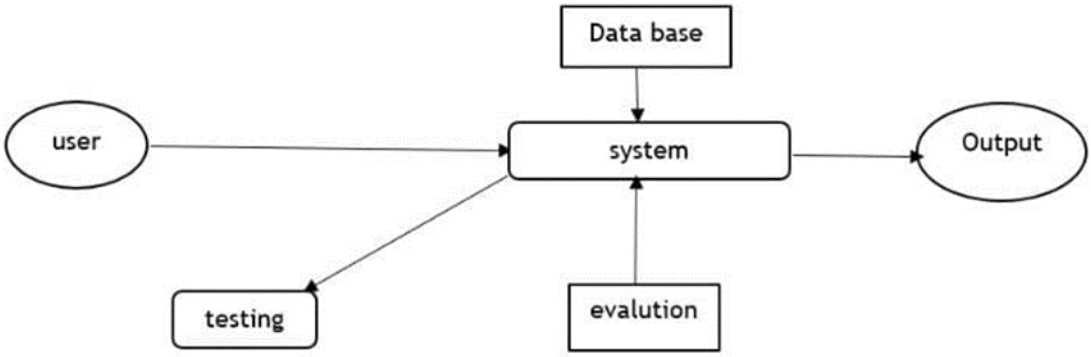

FIGURE : 1 PROPOSED ARCHITECTURE

F. ALGORITHMS USED

Decision Tree

Decision tree is the most powerful and popular tool for classification and prediction. A Decision tree is a flowchart like tree structure, where each internal node denotes a test on an attribute, each branch represents an outcome of the test, and each leaf node (terminal node) holds a class label.

G. IMPLEMENTATION PROCESS

Firstly, we have collected DDOS related datasets.Later we will load the collected dataset to our working environmental necessary pre-processing steps will be completed here before building our required model.Dividing the data into training and testing splits,perform building machine learning model in a flask environment using python.The model has been build with randomforest,designed as, the system delivers the prediction results to the user depending on the inputs entered.

IV. EXPERIMENTAL ANALYSIS

Figure : 2 Main Page

Figure : 3 The Information Uploaded

Figure : 4 Result of the Application

V. CONCLUSION

In ransomware software this software helps to detect weather there is an malware are not and helps to store the data sets related to the data decision tree algorithm also helps to clear the unwanted data that is not related to the project . The project has been done successfully to detect DDoS attacks in this application. This is created in a user-friendly environment with Python programming and Flask. The system is likely to gather data from the user in order to determine whether or not the network is attacked.

Detection and comparitive analysis of ransomware can be utilized in the future to identify numerous attacks could be added to this application in the future. We intend to investigate prediction approach with the revised data set and employ the most accurate and relevant machine learning algorithms for detection.

VI. REFERENCES

[1] . Dong, S., & Sarem, M. (2019). DDoS Attack Detection Method Based on Improved KNN With the Degree of DDoS Attack in Software-Defined Networks. IEEE Access, 8 pp. 5039-5048.

[2]. Dong, S., Abbas, K., & Jain, R. (2019). A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments. IEEE Access, 7, pp. 80813- 80828.

[3]. Gu, Y., Li, K., Guo, Z., & Wang, Y. (2019). Semisupervised K-means DDoS detection method using hybrid feature selection algorithm. IEEE Access, 7, pp.64351- 64365.

[4]. Meti, N., Narayan, D. G., & Baligar, V. P. (2017, September). Detection of distributed denial of service attacks using machine learning algorithms in software defined networks. In 2017 international conference on advances in computing, communications and informatics (ICACCI) IEEE pp. 1366-1371.

[5]. 15th International Symposium on Pervasive Systems, Algorithms and Networks IEEE DDoS Attack Identification and Defense using SDN based on Machine Learning Method, 2018 pp. 5432-5433

[6]. Muthamil Sudar, K., & Deepalakshmi, P. (2020). A two level security mechanism to detect a DDoS flooding attack in software-defined networks using entropy-based and C4. 5 technique. Journal of High Speed Networks, pp, 1- 22.

[7]. Deepa, V., Sudar, K. M., & Deepalakshmi, P. (2018, December). Detection of DDoS attack on SDN control plane using Hybrid Machine Learning Techniques. In 2018 International Conference on Smart Systems and Inventive Technology (ICSSIT) IEEE pp. 299-303 .

[8]. Deepa, V., K. Muthamil Sudar, and P. Deepalakshmi. "Design of Ensemble Learning Methods for DDoS Detection in SDN Environment." 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking ViTECoN, IEEE pp . 780-784 .

[9]. J. Cui, M. Wang, and Y. Luo, ``DDoS detection and defense mechanism based on cognitive-inspired computing in SDN," Future Gener. Comput. Syst., vol. 97, , Aug. 2019 pp. 275-283 .

[10].N. I. G. Dharma, M. F. Muthohar, J. D. A. Prayuda, K. Priagung, and D. Choi, ``Time-based DDoS detection and mitigation for SDN controller," in Proc. 17th Asia_Paci_c Netw. Oper. Manage. Symp. (APNOMS), Aug. 2015, pp. 550-553.

[11] Alexander Adamov; Anders Carlsson(2020),"Reinforcement Learning for Anti-Ransomware Testing") IEEE pp. 989-992.

[12] G Cusack, O Michel and E. Keller(2019), "API Call Based Ransomware Dynamic Detection Approach Using TextCNN". International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE) IEEE pp.4567-4570

[13] Jack W. Stokes; Karthik Selvaraj; Mady Marinescu(2017), "Attention in Recurrent Neural Networks for Ransomware Detection" IEEE pp. 897-992

[14] Jagmeet Singh Aidan, Harsh Kumar Verma, Lalit Kumar Awasthi(2017), "Comprehensive Survey on Petya Ransomware Attack" International Conference on Next Generation Computing and Information Systems (ICNGCIS) IEEE pp. 5678-5679 .