IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.12544

DENIAL OF SERVICE DETECTION OF DISTRIBUTED ATTACKS IN SDN USING MACHINE LEARNING

DIVYA.M[1], RAKESH.P[2], KARTHIKEYAN.K[3], SHAMSUNDAR.R[4],

Dr. N. KOTTISWARAN, M.E., Ph.D[5], Dr. P.D.R VIJAYAKUMAR, M.E.,Ph.D.[6],

Mrs.P . GOKILA, M.E.[7], Mr.K. MADESWARAN, M.E[8]

Info Institute of Engineering, Coimbatore[1-4]

Principal, Info Institute of Engineering, Coimbatore[5]

Professor, Head of the Department, Department of Computer Science and Engineering[6]

Assistant Professor, Department of Computer Science and Engineering[7]

Guide, Assistant Professor, Department of Information Technology[8]

Abstract: Software-defined network (SDN) is a network architecture that used to build, design the hardware components virtually. We can dynamically change the settings of network connections. In the traditional network, it's not possible to change dynamically, because it's a fixed connection. SDN is a good approach but still is vulnerable to DDoS attacks . The DDoS attack is menacing to the internet. To prevent the DDoS attack, the machine learning algorithm can be used. The DDoS attack Is the multiple collaborated systems that used to target the particular server at the same time. In SDN control layer is in the center that link with the application and infrastructure layer, where the devices in the infrastructure layer controlled by the software. In this paper, we propose a machine learning technique namely Decision Tree to detect malicious traffic. Our test outcome shows that the Decision Tree detects whether the attack is safe or not.

I. INTRODUCTION

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic.

Exploited machines can include computers and other networked resources such as IoT devices. From a high level, a DDoS attack is like an unexpected traffic jam clogging up the highway, preventing regular traffic from arriving at its destination. DDoS attacks are carried out with networks of Internet-connected machines.

OBJECTIVE

In SDN architecture, it is possible to reconfigure the multiple devices at the same time. The application layer is used to configure network devices. The control layer (control plane) which consists of the same controller it is the brain of the SDN architecture. These two layers are communicated through API. The infrastructure layer (data plane) that communicates between the controller and the network devices use a central protocol.

REVIEW

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 Defined Networking (SDN) 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

DOI: 10.17148/IJARCCE.2023.12544

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.

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 industry. However, widespread acceptance of these novel networking paradigms has been hampered by the security threats. Advances in the 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 firewallsIn this paper, we present the state of art of the DDoS attacks in SDN and cloud computing scenarios. Especially, we focus on the analysis of SDN and cloud computing architecture.

2.1.6. 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, (Preprint), 1- 22.

Nowadays, many companies and/or governments require a secure system and/or an accurate intrusion detection system (IDS) to defend their network services and the user's private information. In network security, developing an accurate detection system for distributed denial of service (DDoS) attacks is one of challenging tasks. DDoS attacks jam the network service of the target using multiple bots hijacked by crackers and send numerous packets to the target server. Servers of many companies and/or governments have been victims of the attacks. In such an attack, detecting the crackers is extremely difficult, because they only send a command by multiple bots from another network and then leave the bots quickly after command execute. The proposed strategy is to develop an intelligent detection system for DDoS attacks by detecting patterns of DDoS attack using network packet analysis and utilizing machine learning techniques to study the patterns of DDoS attacks. In this study, we analysed large numbers of network packets provided by the Centre for Applied Internet Data Analysis and implemented the detection system using a support vector machine with the radial basis function (Gaussian) kernel. The detection system is accurate in detecting DDoS attacks.

Summary: Muthamil Sudar, K., & Deepalakshmi, P built a method using a support vector machine with the radial basis function (Gaussian) kernel after analyzing huge numbers of network packets given by the Centre for Applied Internet Data Analysis.

III MODULES

The implementation is divided into the following modules:

- User
- System

User:

- Upload Dataset **:** User needs to upload the dataset.
- View Dataset **:** User has ability to view the dataset.
- Input Values for Prediction **:** User needs to enter the input fields required to the system

System:

- Take the dataset **:** System works with the dataset provided to it for model building.
- Preprocessing **:** In preprocessing step system works with to impute any disorders in the data set and extract the features.
- Training **:** In training phase system generates the model from the dataset by using python modules.
- Generate Results **:** System generates the detection results from the model to the user as either the presented values are attacked or not

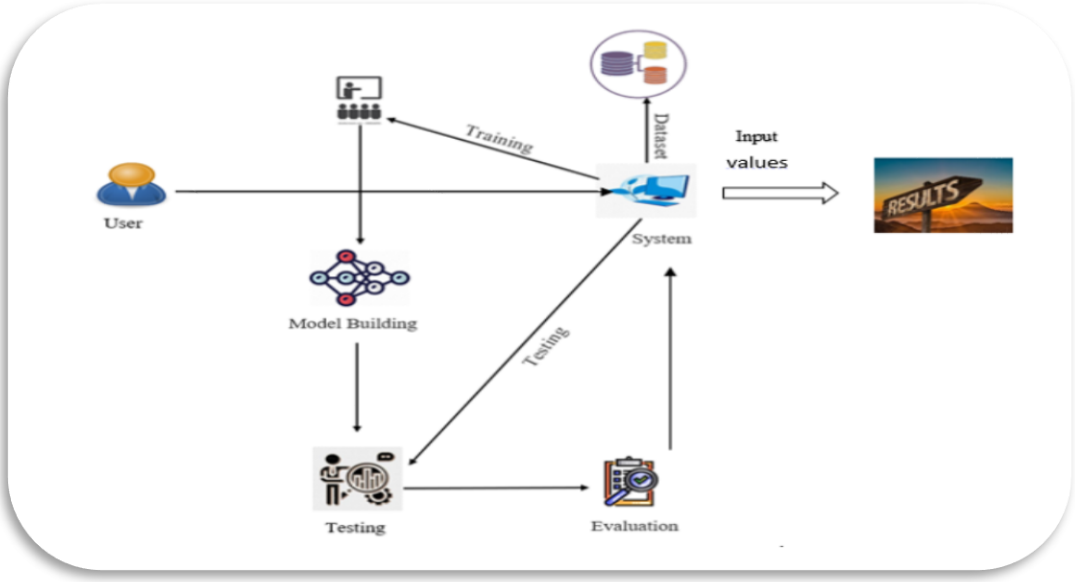
IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

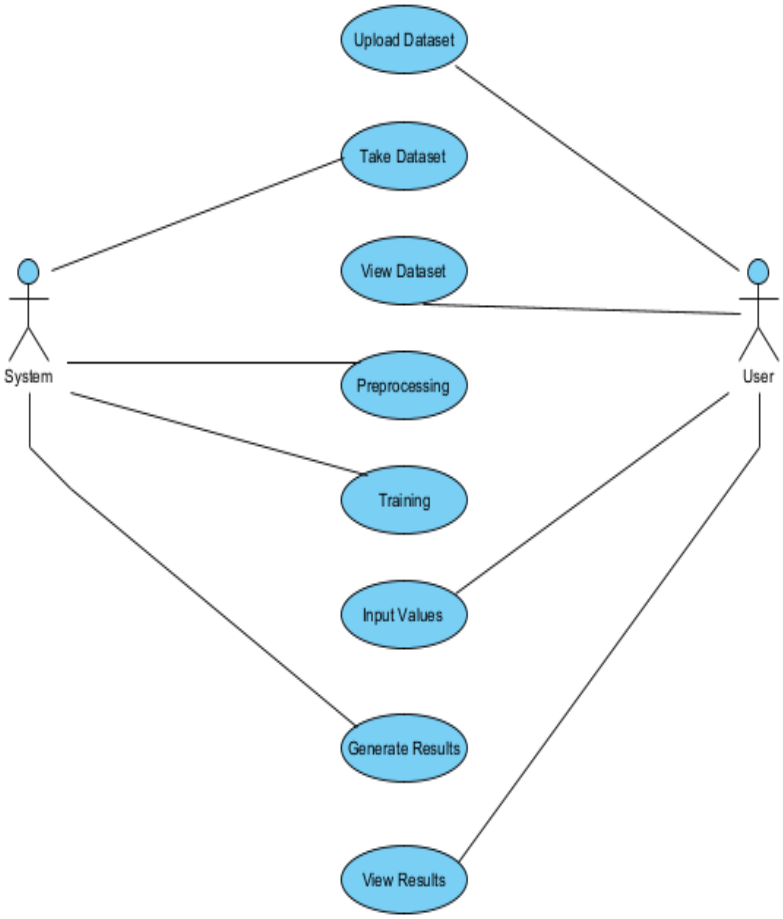
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.12544

ARCHITECTURE DIAGRAMS



USE CASE DIAGRAM



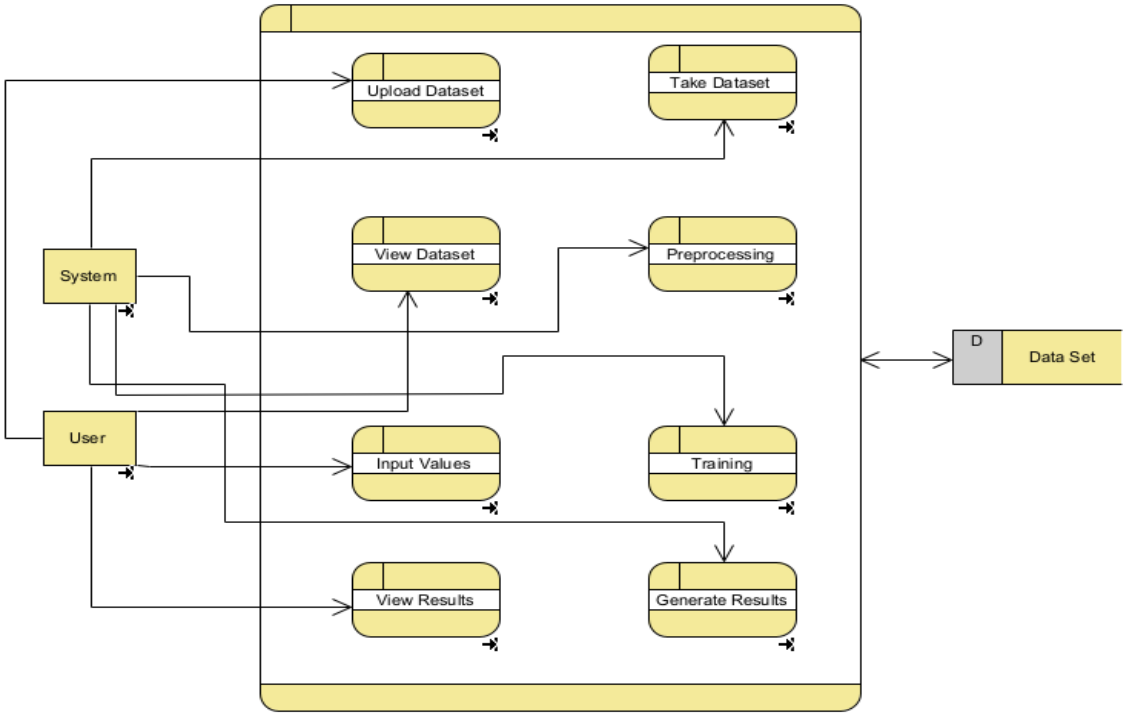
DATA FLOW DIAGRAM

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.12544



IV. RESULTS

- We have successfully developed a system 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 the network is attacked or not.
- The ability 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 detect.

ACKNOWLEDGEMENT

Apart the effort from us, the success of any project depends largely on the encouragement and guideline of many others. We take this opportunity to express our gratitude to the people who have been instrumental in the success completion of this project. We pay our respects and kindly thank our project coordinator **Mrs.P .GOKILA,M.E .,** Assistant Professor, Department of Computer Science and Engineering, for his valuable guidance and timely suggestion inbringing out this project. We pay indebtedness to our project guide **Mr.K.MADESWARAN, M.E.,**Assistant Professor, Department of Information Technology, for his valuable guidance and timely suggestion in bringing out this project.

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, 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, 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, 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) (pp. 1366-1371). IEEE.
5. 15th International Symposium on Pervasive Systems, Algorithms and Networks IEEE DDoS Attack Identification and Defense using SDN based on Machine Learning Method, 2018
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, (Preprint), 1-22.