IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, February 2024

DDOS Attack Detection

Dhananjay Tangtode[1], Shayan Sayyad[2], Omkar Gelye[3], Sarthak Sawant[4], Prof. Girisha Bombale[5]
Students, Department of Artificial Intelligence and Data Science Engineering
Professor, Department of Artificial Intelligence and Data Science Engineering
Shree Ramchandra College of Engineering, Pune, Maharashtra, India
dhananjaytangtode@gmail.com, sayyadshayan49@gmail.com, omkargelye221@gmail.com,
sawantsarthak12@gmail.com, girishabombale@gmail.com.

Abstract: *A Distributed Denial of Service (DDoS) attack is an attempt to make a service unavailable by overwhelming the server with malicious traffic. DDoS attacks have become the most tedious and cumbersome issue in recent past. The number and magnitude of attacks have increased from few megabytes of data to 100s of terabytes of data these days. Due to the differences in the attack patterns or new types of attack, it is hard to detect these attacks effectively. In this paper, we devise new techniques for causing DDoS attacks and mitigation which are clearly shown to perform much better than the existing techniques. We also categorize DDoS attack techniques as well as the techniques used in their detection and thus attempt an extensive scoping of the DDoS problem. We also compare our attack module with a couple of tools available.*

Keywords: ML, Smart, Grid, PCA, SVM algorithm, Computer aided diagnosis, Dos attack

I. INTRODUCTION

The industrial industry is undergoing a dramatic transition as a result of the information era. In this context, the notion of smart grid arose as the times demanded, and it has since gained widespread recognition on a global scale, becoming a common development trend in the global power business. However, there have been instances of smart grid intrusion in the past. On January 6, 2016, for example, hackers attacked the Ukrainian electricity grid infrastructure, forcing hundreds of houses to turn off their lights. This is the first time in history that a cyber-attack has resulted in power interruptions. This cyber-attack on industrial control systems is unquestionably a watershed moment.

II. ARCHITECTURE

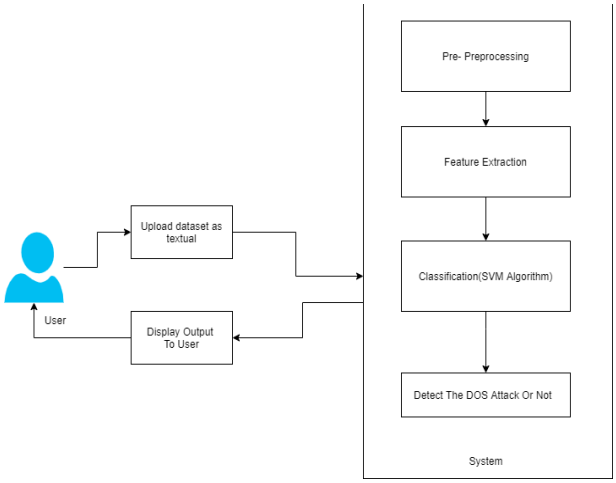


Figure 1: System Architecture

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, February 2024

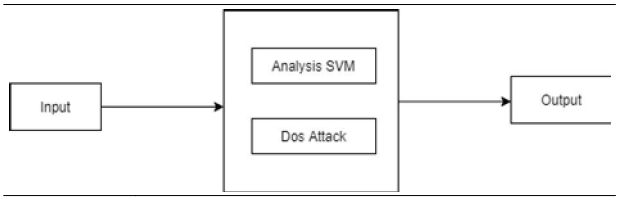


Figure 2: Data Flow Diagram

III. IMPLEMENTATION

In an SDN, attacks can occur either on the data plane or control plane. Attacks on the former are similar to traditional attacks and affect a few hosts. However, attacks on the latter attempt to bring down the entire network. In this second kind of attack, adversaries fingerprint an SDN for flow installation rules and then send new traffic flows, resulting in flow table-misses in the switch. This phenomenon forces the controller to handle every packet and install new flow rules in switches that consume system resources on the controller and switches. In our previous work, we empirically evaluated the impact of SDN adversarial attacks on network services.

In the current work, we implement a DDoS detection system as a network application in SDN to handle attacks for both cases

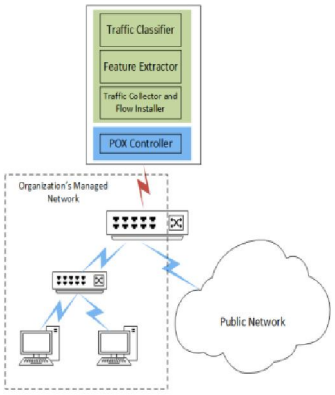
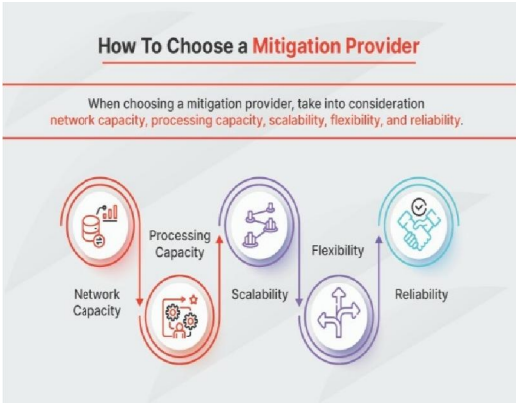


Figure 3: Implementation Plan



IV. ALGORITHM

First we will provide image dataset to the machine dataset of images of currency. Then the data processing phase, in this removing the noisy and blur part of dataset, and resize the image dataset. After preprocessing of dataset, next phase is trained that dataset. For that, dataset goes through feature extraction classification.

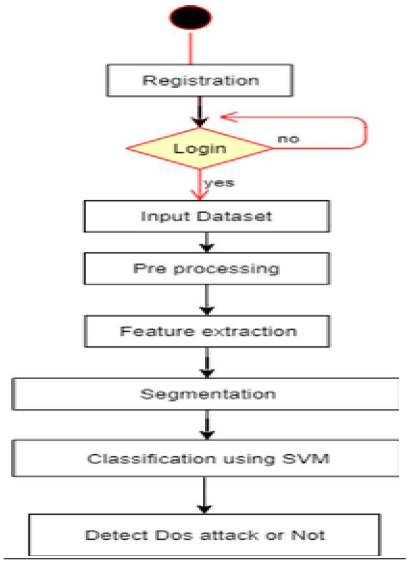
IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, February 2024

Train the dataset, In this process the training of dataset is done by following steps. 1) Feature extraction extract the features like edge, size etc. From dataset. Extract the features for classification.

The next step is of testing, in this the input as image is given to the system. Then Model can goes to testing phase and then provide the output to user. Output is detect the currency is fake or not.

The next step is of classification in this the SVM algorithm is used. "Support Vector Machine" is a supervised machine learning algorithm that can be used for both classification or regression challenges.

V. ACTIVITY DIAGRAM



VI. ADVANTAGES

1 Easy to handle.
2. Improve Best accuracy.
3. Increase the knowledge about security.
4. Can leverage the greater volume of machine to execute a seriously disruptive attack.
5. The Location of the attack is difficult to detect due to the random distribution of attacking system.

VII. LIMITATIONS

1.Genuine users are not able to access resources, so may not be able to find the information or carry out the action they need.
2. Businesses may not be able to carry out time critical action.
3. They may suffer reputational damage.
4. Customers may choose to use a competitor.

VIII. CONCLUSION

This work provides a smart grid Dos attack detection methodology based on machine learning to address the challenge of smart grid intrusion detection. In real time, the approach gathers network communication data between the smart meter and the data server.

1) Training the data using SVM algorithm.
2) The Convolutional Neural network is used to classification.
3) KDD99 dataset is used to train data.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, February 2024

REFERENCES

[1] S. RoselinMary, M. Maheshwari, M. Thamaraiselvan
Early Detection of DOS Attacks in VANET Using Attacked Packet Detection Algorithm (APDA)
[2] Faisal Hussain, SyedG hazanfar Abbas, Muhammad Husnain, Ubaid U. Fayyaz, Farrukh Shahzad, Ghalib A. Shah. Iot Dos and DDOS attack detection using ResNet.
[3] Faisal Mochamad Teguh Kurniawan, Setiadi Yazid Abdelrhman Mohammed, Iman Abuel Maaly Abdelrahman. Mitigation and Detection Strategy of DoS Attack on Wireless Sen_x0002_sor Network Using Blocking Approach and Intrusion Detection System.
[4] Xiang-GuiGuo, Xiao Fan, Jian-Liang Wang, and Ju H. Park. Event-triggered Switching-type Fault Detection and Isolation for Fuzzy Control Systems under DoS Attacks.
[5] Mohiuddi Ahmed Thwarting DoS Attacks: A Framework for Detection based on Collective Anomalies and Clustering