Detection & Mitigation of DDOS Attack

Muhammad Zulkifl Hasan (Zulkifl.hasan@ucp.edu.pk)
University of Central Punjab
Muhammad Zunnurain Hussain
Bahria University Lahore Campus
Muhammad Zeeshan Nazar
University of Central Punjab
Mahelak A
University of Central Punjab
Fatima Anjum
University of Central Punjab
Muhammad Atif Yaqub
National College of Business Administration and Economics
Muzzamil Mustafa
National College of Business Administration and Economics
Saad Hussain Chuhan
National College of Business Administration and Economics
Zaima Mubarak
National College of Business Administration and Economics
Adeel Ahmad Siddiqui
National College of Business Administration and Economics
Ali Moiz Qureshi
National College of Business Administration and Economics
Dr Ghulam Mustafa
Bahria University Lahore Campus

Research Article

Keywords: DDoS, cloud, network, traffic, malicious, threat, attack, detect, mitigate

Posted Date: February 16th, 2023

DOI: https://doi.org/10.21203/rs.3.rs-2586448/v1

Additional Declarations: No competing interests reported.

Detection & Mitigation of DDOS Attack

Muhammad Zulkifl Hasan[1*], Muhammad Zunnurain Hussain[2], Dr Ghulam Mustafa[3] , Muhammad Zeeshan Nazar[4], Mahelaka[5], Fatima Anjum[6] ,Muhammad Atif Yaqub[7], Muzzamil Mustafa[8], Saad Hussain Chuhan[9], Zaima Mubarak[10], Adeel Ahmad Siddiqui[11], Ali Moiz Qureshi[12]

[1,4,5,6]Faculty of Information Technology University of Central Punjab, Lahore, 54000, Pakistan

[2,3]Department of Computer Science, Bahria University Lahore Campus, Lahore, 54000, Pakistan

[7-12]Department of Computer Science National College of Business Administration and Economics, Lahore, Pakistan

[*]Corresponding Author: Muhamamd Zulkifl Hasan. Email: Zulkifl.hasan@ucp.edu.pk

***Abstract*—**

The DDoS (Distributed Denial of Service) attack is a type of Cyberattack in which multiple attackers aim to attack different network resources like a server or a website. Although many statistical methods have already been designed for DDoS attack detection, designing a real-time detector with low computational overhead is still one of the main concerns. The already existing datasets are highly important and can be used for constructing and checking new solutions. It is the most dangerous attack against IPv6 networks today. The attack uses Internet Control Message Protocol version 6 (ICMPv6) messages. DDoS attack can be detected in various ways like a sudden fluctuation in the traffic of a website or unreal raise in the requests to resources. DDoS attacks are among the four most malicious attacks, like social engineering, ransomware, and supply chain attacks. It's relatively easy to confuse DDoS attacks with other cyber threats. As for now most of our application and infrastructure resides on the cloud. As for cloud providers, the services provider must facilitate some tools to prevent the attack on their services and their user. Some of the major cloud providers give us this type of facility (AWS, Azure, and GCPThis cloud service provider offers cloud DDoS mitigation and prevention that operates entirely outside of your current network, inside the Internet cloud, and can identify and stop DDoS attacks before they even get to you. For bigger installations, routing is utilised to ensure that all network traffic, regardless of type, is filtered before delivery via a clean pipe. Domain name system (DNS) is used to direct inbound traffic through a scrubbing centre before delivery to the server. DDoS mitigation and prevention in the cloud is not only speedy, but also incredibly effective at stopping DDoS attacks.

Keywords—DDoS, cloud, network, traffic, malicious, threat, attack, detect, mitigate (key words)

I. INTRODUCTION

A. The DDoS (Distributed Denial of Service) attack is a type of Cyberattack in which multiple attackers aim to attack different network resources like a server or a website. Like any other attack, DDoS is made possible by exploitation of vulnerabilities. It is done by disrupting the flow of the traffic. It is a non-intrusive attack, which means that the attacker does not require admin access to the resources to attack. DDoS is used to attack on devices connected to the internet.

B. A bot or a collection of many bots, known as botnet are used to overwhelm the server or the website. When many requests are sent at a time, the resources will not be able to operate properly as they have a limitation and require processing time to provide the services. This way, the normal traffic can be deprived of its right to the services which explains the Denial of Services part of DDoS.

C. The Distributed part of Distributed Denial of Services attack is a difference from DOS (Denial of Services) attack. The attack is launched from different compromised devices distributed at various parts of the network all over the world. Each bot in a botnet is a legitimate device having a legitimate IP address on the Internet, which is why separating the malicious traffic from the real one is a difficult task.

II. DISTINCTION OF DDOS FROM DOS

A. The main difference in DDoS in DOS is that in DOS (Denial of Service) attack, a single device or network is used to launch the attack, whereas in in DDoS (Distributed Denial of Services) attack, the attack is launched through different sources.

B. Each bot in a botnet is a legitimate device having a legitimate IP address on the Internet, which is why separating the malicious traffic from the real one is a difficult task.

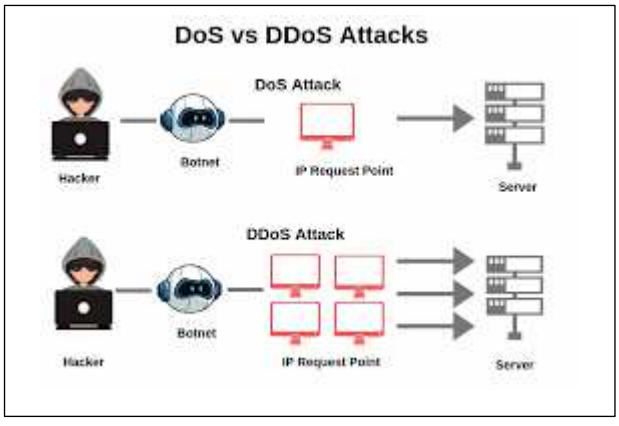


Fig 1 – Diagram Showing Difference Between DDoS and Dos Attacks

III. WORKING OF DDOS

A. A flood of requests is generated by different sources. These can be multiple devices attacked by malware and compromised to attack a target which is on the Internet.

B. This flood of attack distrupts the traffic flow of the targetted resource and causes a denial of srvices like email, websites, e-commerce sites.

C. The compromised devices used to launch the attack are known as bots and a group of bots make up a botnet. Since each bot is a compromised device on the Internet, it has a legitimitate IP address so it is very difficult to detect or separate from the normal traffic.

D. Once the targetted resource is saturated with overwhelming amount of requests, it can no longer provide its services to the authorised or normal traffic as well because it does not have the capactiy to process so many requests. It is kind of like a jam in the traffic.

Fig 2 – Server Attacked Using DDoS

IV. DETECTION OF DDOS ATTACK

A. Since DDoS (Distributed Denial of Services) attack can be caused by bots using legitimiate IP addresses, it can be detected if there is an unreal or suspicious amount of traffic from a single source or IP.

B. Another tell can be a sudden rise in the requests for a speciifc resource, like a website, or a server.

C. The abnormal traffic can be detected by checking the spikes at specific times of a resource. If there is a strange change in the usual flow, it might be because of a DDoS attack.

V. TYPES OF DDOS ATTACK

As DDoS (Distributed Denial of Service) attack focuses on attacking the IOT (Internet of Things) resources, different types of DDoS (Denial of Services) attacks target different layers in the OSI (Open System Interconnection) model.

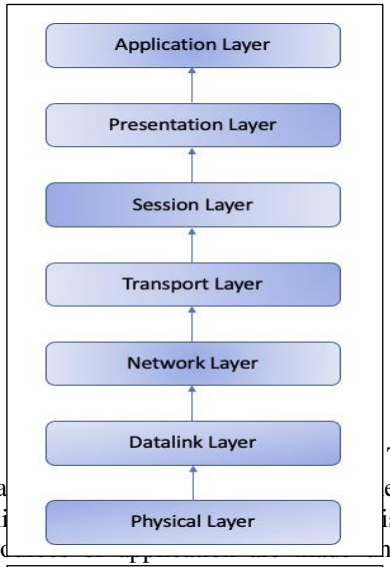


Fig 3 – OSI Model

A. This is the atta e OSI Model whi is attack, the res available to legi esources are consumed by sending a flood of requests for the usage of these resources.

1. HTTP Flood Attack: It is a type of Application Layer Attack in which many HTTP requests are sent over and over flooding the server.

B. Protocol Attacks / State Exhaustion Attacks: This attack is done on the 3rd and 4th layer of the OSI (Open System Interconnection) Model that are Network Layer, and Trasnport Layer respectively. In this attack the network resources like the server or other equipment like firewalls or load balancers of the attacked source are over consumed.

1. SYN Flood: It is a type of attack in which a huge amount of "Initial Connection Requests" SYN packets of a TCP handshake are sent by the attacker.

This technique uses a spoofed source's IP address.

C. Volumetric Attacks: Volumetric attacks work by robbing the target's bandwidth. All the bandwidth between the target and the Internet is sucked up by sending a large amount of data or using amplification or creating a lot of traffic through other means.

1. DNS Amplification: It is a type of attack in which the target's IP is used. The attacker creates a spoofed IP which is actually the IP address of the targetted source, and then the target's IP is made to receive a massive amount of responses from the server.

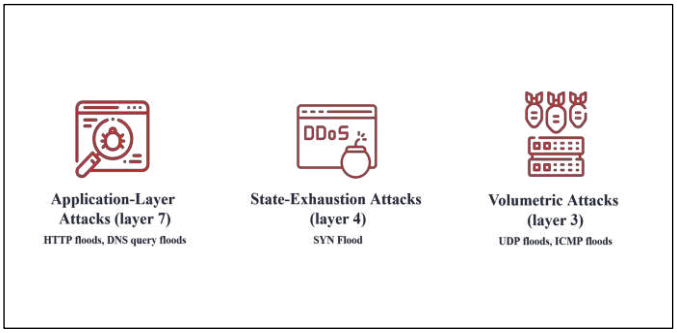


Fig 4 - Types of DDoS Attacks

VI. HAZARDS OF DDOS ATTACKS

DDoS (Distributed Denial of Services) attacks are not only difficult to identify but also difficult to deal with. As the attacker uses techniques that make it hard to identify the malicious traffic from the normal traffic, it can cause a lot of damage. In various businesses, it can become a cause of a huge loss as businesses cannot risk having to block all of the traffic to their resources. There are various methods that are used to prevent or mitigate the attacks.

A. Can Firewalls Be Used?

Unfortunately, firewalls can also become the victim of these attacks which is why they are not effective in filtering out the malicious traffic from the authorized or normal traffic. So, they cannot be used alone to deal with the hazards of DDoS attacks. In fact, load balancers or any other types of IPS (Intrusion Prevention System) devices cannot be used to ensure network availability.

B. DDoS On Cloud: Many organizations now use cloud computing which is why DDoS attacks has become of the most common types of attacks done on cloud computing as well.

VII. MITIGATION OF DDOS ATTACKS

Dealing with DDoS can be difficult. There are tools that are used to prevent or mitigate the DDoS attacks. These services depend on various factors like:

1. Scalability: As the businesses and DDoS both can grow, the services should be able to scale according to the need.
2. Flexibility: In order to keep the site running, a real-time check of incoming threats is important. Flexibility is required to keep the incoming threats in check and to deal with them.
3. Realibility: Whenever there is a threat of a DDoS (Distributed Denial of Services) attack, the mitigating services should be available right on time and should function properly.
4. Network Size: The size of the network contributes to the functioning of a mitigating services. Larger the size of network, quicker the response of the mitigating service.

VIII. PREVENTION OF DDOS ON CLOUD

A. One approach to prevent DDoS attacks on the cloud is the use of a cloud-based DDoS protection service. These services use a combination of hardware and software, such as firewalls, intrusion detection, and prevention systems, and traffic analyzers, to identify and filter out malicious traffic before it reaches the targeted server or network. These services can also provide real-time monitoring and reporting, as well as automatic blocking of suspicious traffic. Studies have shown that cloud-based DDoS protection services can effectively detect and mitigate DDoS attacks, and can significantly reduce the impact of an attack on the targeted resources.

B. As we can use a content delivery network (CDN) to distribute traffic across multiple servers, making it more difficult for an attacker to overload a single server or network. This approach can also help to reduce the impact of a DDoS attack by spreading the traffic across multiple locations. Studies have shown that CDNs can effectively mitigate DDoS attacks and reduce the impact on the targeted resources.

C. Cloud providers also use the virtual private cloud (VPC) to segment your network and limit the exposure of your resources to the Internet. This can help to reduce the attack surface and make it more difficult for an attacker to locate and target specific resources. Studies have shown that VPCs can effectively mitigate DDoS attacks by limiting the exposure of resources to the Internet and reducing the attack surface.

D. Mitigate DDoS attack is used as a firewall, which can be configured to block or limit traffic from specific IP addresses or ranges, or to limit the number of connections from a single IP address. firewalls can effectively block DDoS attacks by filtering out malicious traffic.

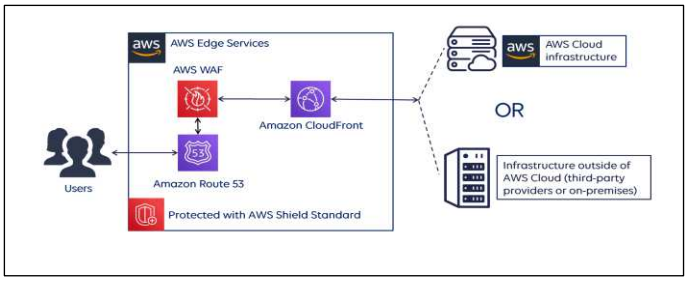


Fig 5 – Example of AWS Cloud

IX. DATASET OF DDOS

A. Data Preprocessing: We have processed the data of the datasets in order to:

1. Drop null values or to drop columns having only one value.
2. Drop categorial columns having one category prominence.
3. Drop columns having more 50% of missing values.
4. Drop rows where column missing values are more than 5%

B. We have used the dataset from kaggle. It has a total of 83 columns

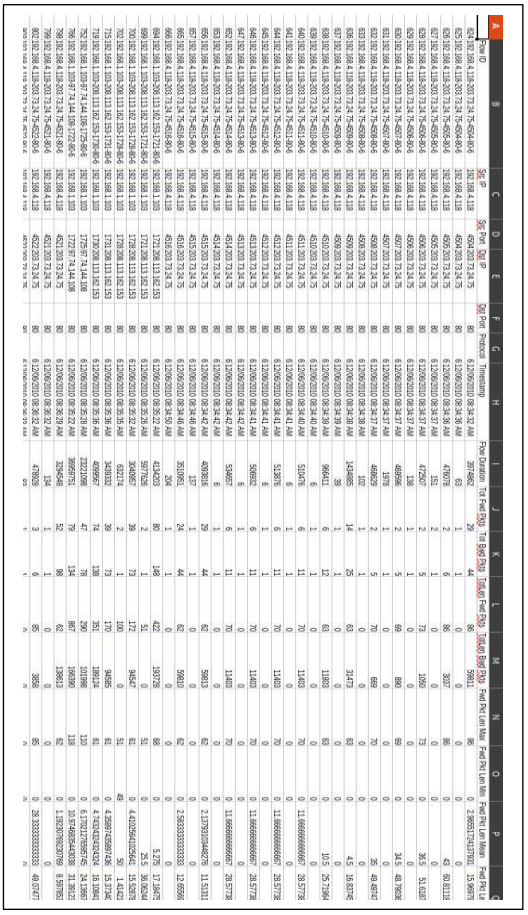


Fig 5 – Dataset of DDoS

C. Reading data from Kaggle DDoS Source CVS

```
df = pd.read_csv(
    '/kaggle/input/ddos-datasets/ddos_balanced/final_dataset.csv
    dtype=dtypes,
    parse_dates=['Timestamp'],
    usecols=[*dtypes.keys(), 'Timestamp'],
    engine='c',
    low_memory=True
)
```

Fig 6 – Code of reading data

D. Dataframe of DDoS CVS

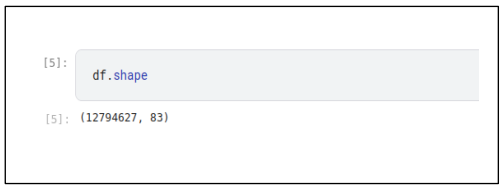


Fig 7 – Data-Frame Shape

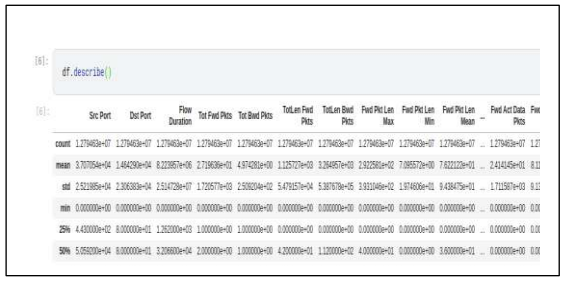


Fig 8 – Describe Data-Frame

E. Dropping columns having only one value.

Fig 9 – Code to drop out columns

F. Dropping categorial columns that have one category predominance.

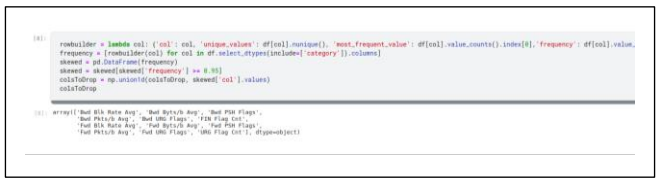


Fig 10 – Code to drop categorial columns

G. Dropping columns that have more than 50% of missing values.

Dropping rows that have columns are missing values more than 5%.

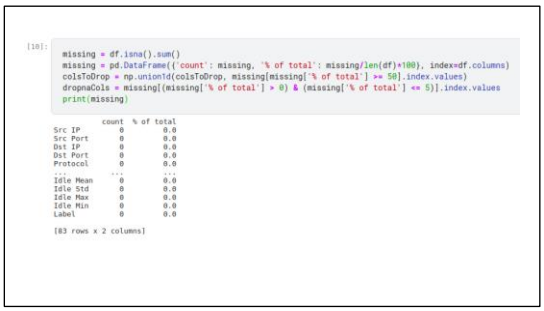


Fig 11 – Code of dropping columns and rows

H. Handling the faulty data.

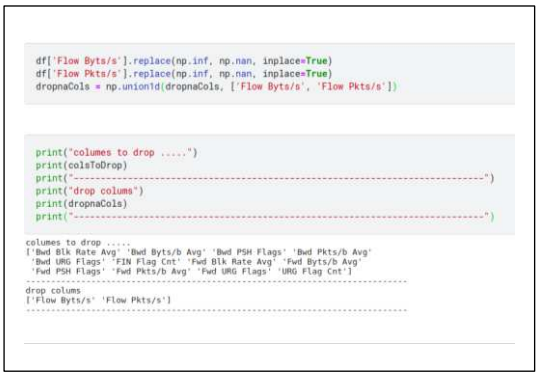


Fig 12 – Code of Handling Faulty Data

I. Dropping columns from the data-frame.

Fig 13 – Code of dropping columns from the data-frame

J. Train testing the data split

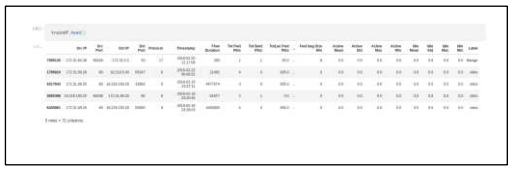


Fig 14 & Fig 15– Train testing data split

X. SCATTER PLOTS

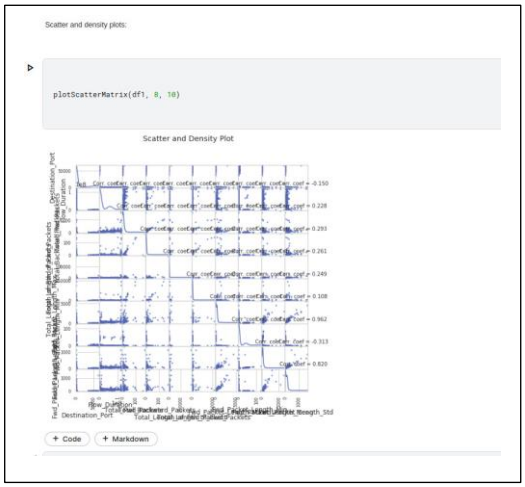


Fig 16 – Scatter and Destiny Plot

XI. DISTRIBUTION GRAPHS (HISTOGRAM/BAR GRAPH) OF SAMPLED COLUMNS:

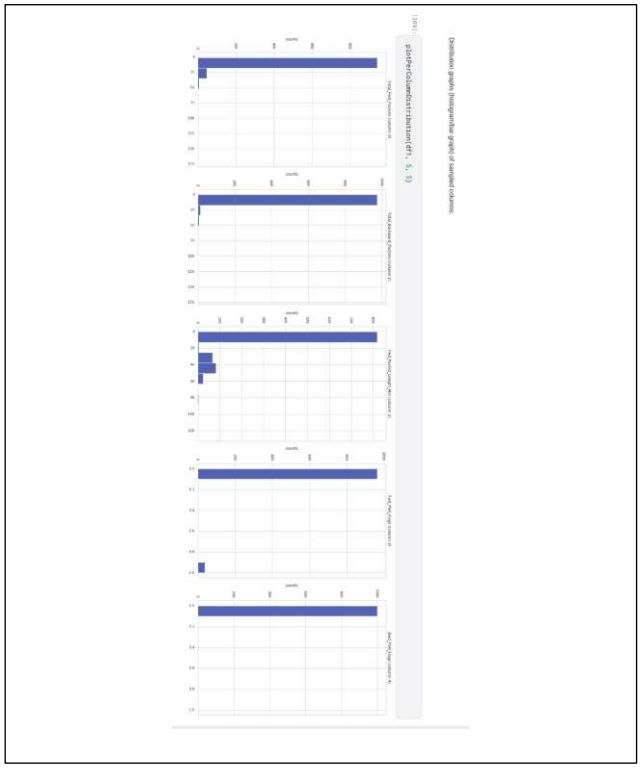


Fig 17 – Distribution Graph

XII. SCATTER PLOT SHOWING BENIGN, DDOS HULK, AND DDOS SLOWLORIS

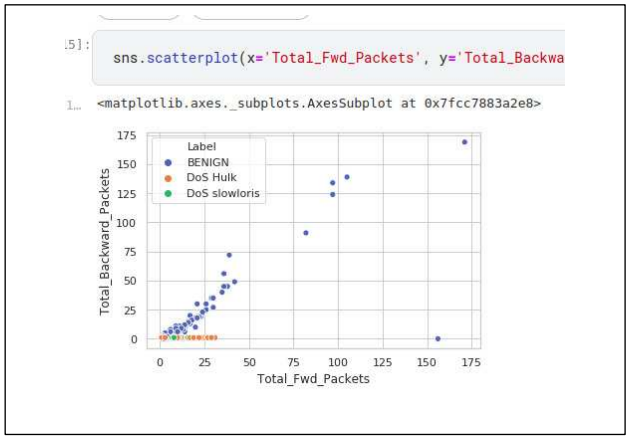


Fig 18 – Scatter Plot

XIII. BAR PLOT

```
# plotting the target variable
labelCount = df1['Label'].value_counts(normalize=True)*100
ax = sns.barplot(x=labelCount.index, y=labelCount.values)
ax1 = ax.twinx()
ax.set_ylabel('Frequency [%]')
ax1.set_ylabel("Count (in millions)")
ax1.set_ylim(0, len(df1)/10**6)
ax.set_ylim(0, 100)
plt.title('Target Variable')
```

```
Text(0.5, 1.0, 'Target Variable')
```

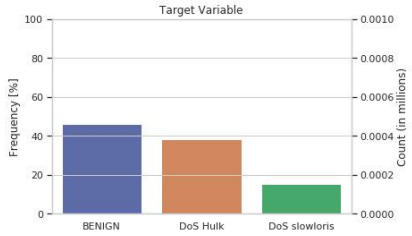


Fig 19 – Bar Plot

```
sns.set(style='whitegrid')

sns.boxplot(x='Total_Fwd_Packets', y='Total_Backward_
```

```
<matplotlib.axes._subplots.AxesSubplot at 0x7fcbf0ec9d30>
```

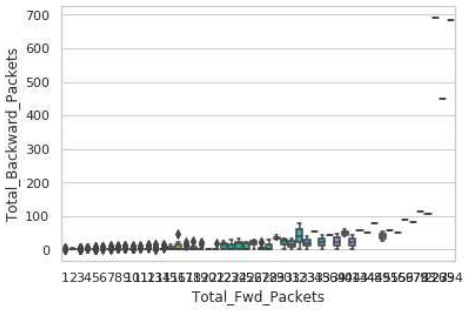


Fig 20 & 21– Box Plots

XIV. BOX PLOT

```
sns.set(style='whitegrid')

sns.boxplot(x='Total_Fwd_Packets', y='Total_Backward_Packets
```

```
<matplotlib.axes._subplots.AxesSubplot at 0x7fcc790ea5f8>
```

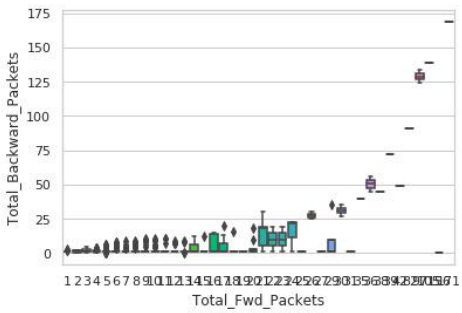
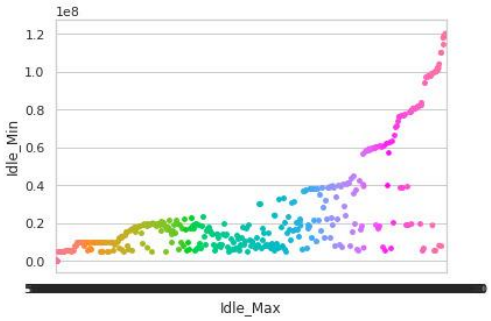


Fig 20 – Box Plot

XV. SWARMP PLOT

```
sns.swarmplot(x ="Idle_Max", y = "Idle_Min",
              data = df1, size = 5)
plt.show()
```




```
sns.swarmplot(x ="Idle_Max", y = "Idle_Min",
              data = train_data, size = 5)
plt.show()
```

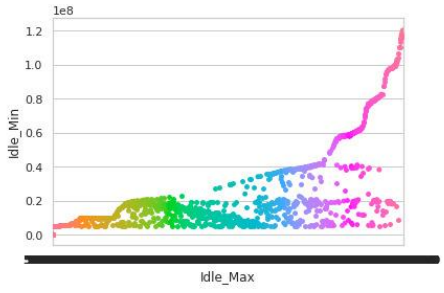


Fig 22 & 23 – Swarm Plots

XVI. PLOT CORRELATION MATRIX

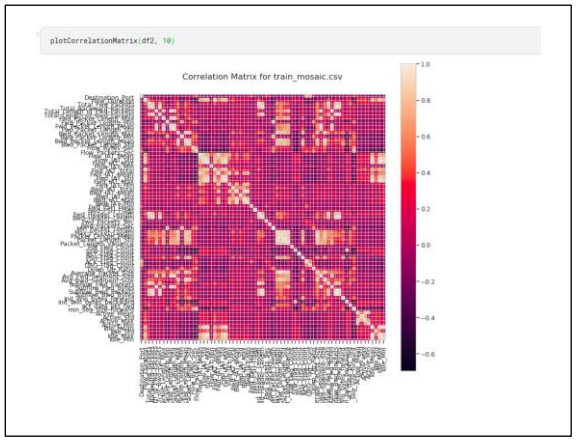


Fig 24 – Plot Correlation Matrix

XVII. VIOLIN PLOT

```
sns.set(style = 'whitegrid')
plt.figure(figsize=(9,6))
sns.violinplot(x ="Total_Fwd_Packets",
               y ="Total_Backward_Packets",
               data = train_data)
plt.show()
```

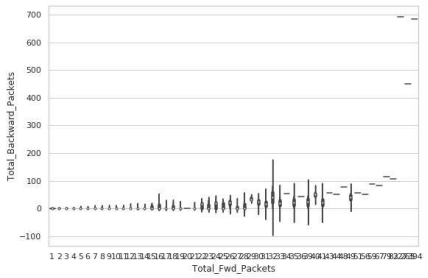
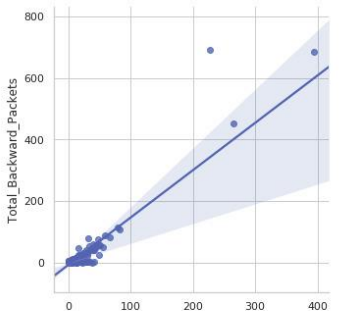


Fig 25 – Violin Plot

XVIII. JOINT PLOT AND JOINT GRID

```
sns.lmplot(x ="Total_Fwd_Packets",
           y ="Total_Backward_Packets",
```

```
<seaborn.axisgrid.FacetGrid at 0x7fcbf1d5def0>
```



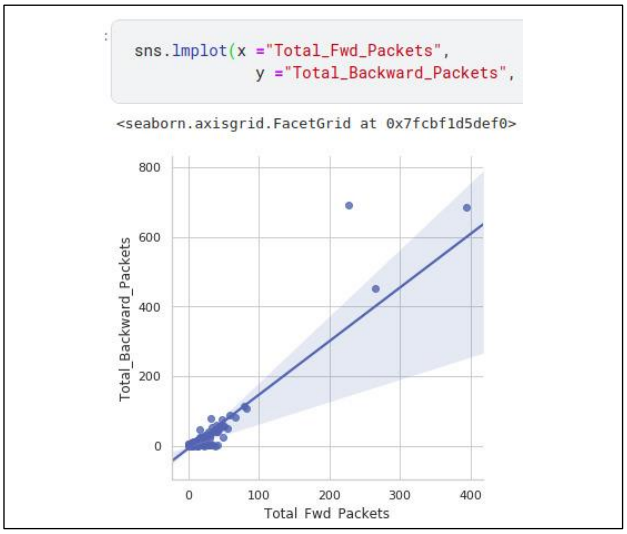
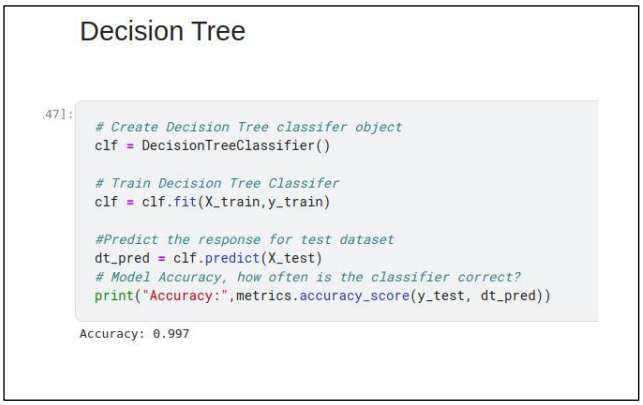


Fig 26 & 27– Joint Plot & Joint Grid

XIX. NAÏVE BAYES ALGORITHM

Fig 28– Naïve Baves Algorithm

XX. DECISION TREE ALGORITHM



XXI. RANDOM FOREST

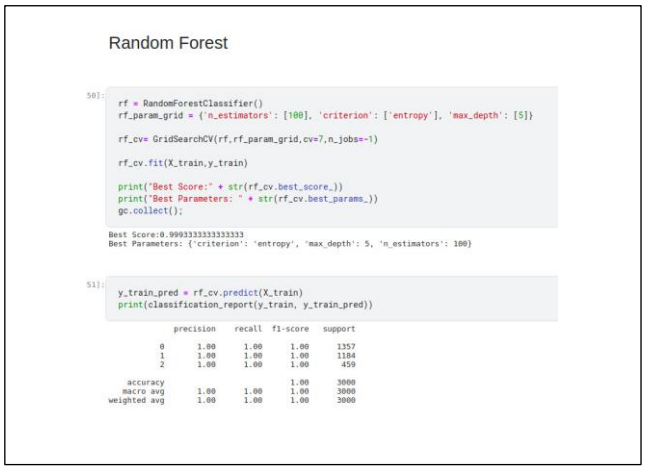


Fig 30– Random Forest

XXII. K NEIGHBORS

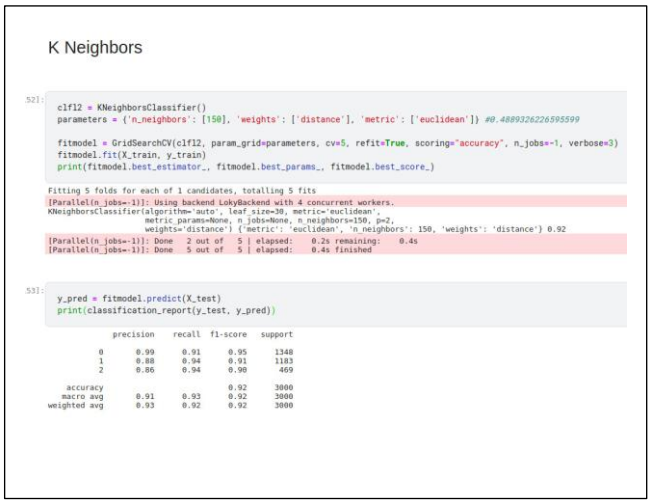


Fig 31– K Neighbor

XXIII. 1D CONV

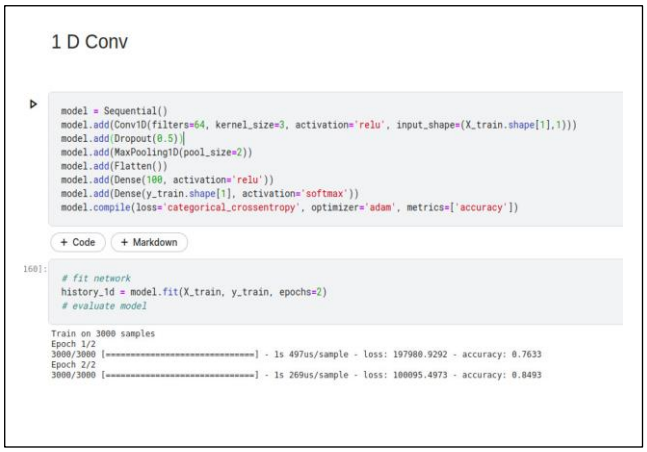
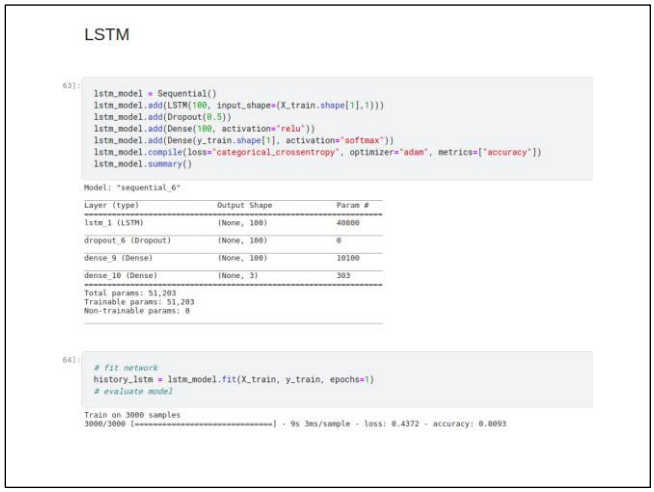
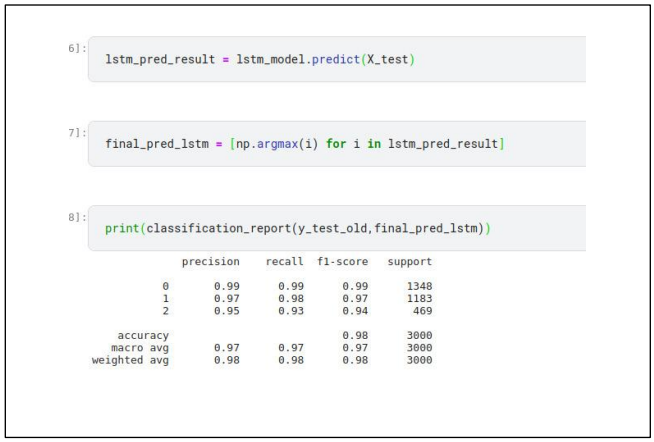


Fig 32– 1D Conv

XXIV. LSTM





```
[62]: pred_result = model.predict(X_test)
      final_pred = [np.argmax(i) for i in pred_result]
      print(classification_report(y_test_old,final_pred))

                    precision    recall  f1-score   support

                 0       0.84      0.96      0.90      1348
                 1       0.88      0.78      0.82      1183
                 2       0.91      0.80      0.85       469

          accuracy                           0.86      3000
         macro avg       0.88      0.85      0.86      3000
      weighted avg       0.87      0.86      0.86      3000
```

Fig 33, 34, and 35 – LSTM

XXV. CONCLUSION

In conclusion, various methods can be used to prevent DDoS attacks on cloud-based resources, including cloud-based DDoS protection services, content delivery networks, virtual private clouds, firewalls, and regular security updates and monitoring. Each of these methods has been shown to be effective in mitigating DDoS attacks and reducing their impact on targeted resources.

XXVI. REFERENCES

1. *M, S. (2020) DDoS botnet attack on IOT devices, Kaggle. Available at: https://www.kaggle.com/datasets/siddharthm1698/ddos-botnet-attack-on-iot-devices (Accessed: January 29, 2023).*
2. *UNR-IDD Intrusion Detection Dataset (no date) Kaggle. Available at: https://www.kaggle.com/datasets/tapadhirdas/unridd-intrusion-detection-dataset (Accessed: January 29, 2023).*
3. *Attacks and targeted layers in IOT. | download scientific diagram (no date). Available at: https://www.researchgate.net/figure/Attacks-and-Targeted-Layers-in-IoT_fig3_350595140 (Accessed: January 29, 2023).*
4. *Vishwakarma, R. and Jain, A.K. (2019) A survey of ddos attacking techniques and defence mechanisms in the IOT network - telecommunication systems, SpringerLink. Springer US. Available at: https://link.springer.com/article/10.1007/s11235-019-00599-z (Accessed: January 29, 2023).*
5. *Nikhil Tripathi Fraunhofer Institute for Secure Information Technology et al. (2022) Application layer denial-of-service attacks and Defense Mechanisms: A Survey: ACM Computing Surveys: Vol 54, no 4, ACM Computing Surveys. Available at: https://dl.acm.org/doi/abs/10.1145/3448291 (Accessed: January 29, 2023).*
6. *panelB.B.GuptaabcdPersonEnvelopePoojaChaudharyaXiaojunChangeNadiaNedjahf, A.links open overlay et al. (2022) Smart defense against distributed denial of service attack in IOT networks using supervised learning classifiers, Computers & Electrical Engineering. Pergamon. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0045790622000404 (Accessed: January 29, 2023).*
7. *What is a distributed denial-of-service (ddos) attack? - cloudflare (no date). Available at: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ (Accessed: January 29, 2023).*
8. *What is ddos blackhole routing? | cloudflare (no date). Available at: https://www.cloudflare.com/learning/ddos/glossary/ddos-blackhole-routing/ (Accessed: January 29, 2023).*
9. *Why is a ddos attack dangerous? (no date) NETSCOUT. Available at: https://www.netscout.com/what-is-ddos/why-is-ddos-dangerous (Accessed: January 29, 2023).*
10. *What is a volumetric attack? (no date) NETSCOUT. Available at: https://www.netscout.com/what-is-ddos/volumetric-attacks (Accessed: January 29, 2023).*
11. *What is a decision tree (no date) IBM. Available at: https://www.ibm.com/topics/decision-trees (Accessed: February 2, 2023).*
12. *Banoula, M. (2023) Naive Bayes classifier - machine learning [updated]: Simplilearn, Simplilearn.com. Simplilearn. Available at: https://www.simplilearn.com/tutorials/machine-learning-tutorial/naive-bayes-classifier (Accessed: February 2, 2023).*
13. *IBM, "What is Random Forest? | IBM," www.ibm.com. https://www.ibm.com/topics/random-forest*
14. *IBM, "What is the k-nearest neighbors algorithm? | IBM," www.ibm.com. https://www.ibm.com/topics/knn*
15. *"What is LSTM (Long Short Term Memory)," video.ibm.com. https://video.ibm.com/recorded/131507960 (accessed Feb. 01, 2023).*