DDoS Detection using Machine Learning Algorithms

PRESENTED BY:

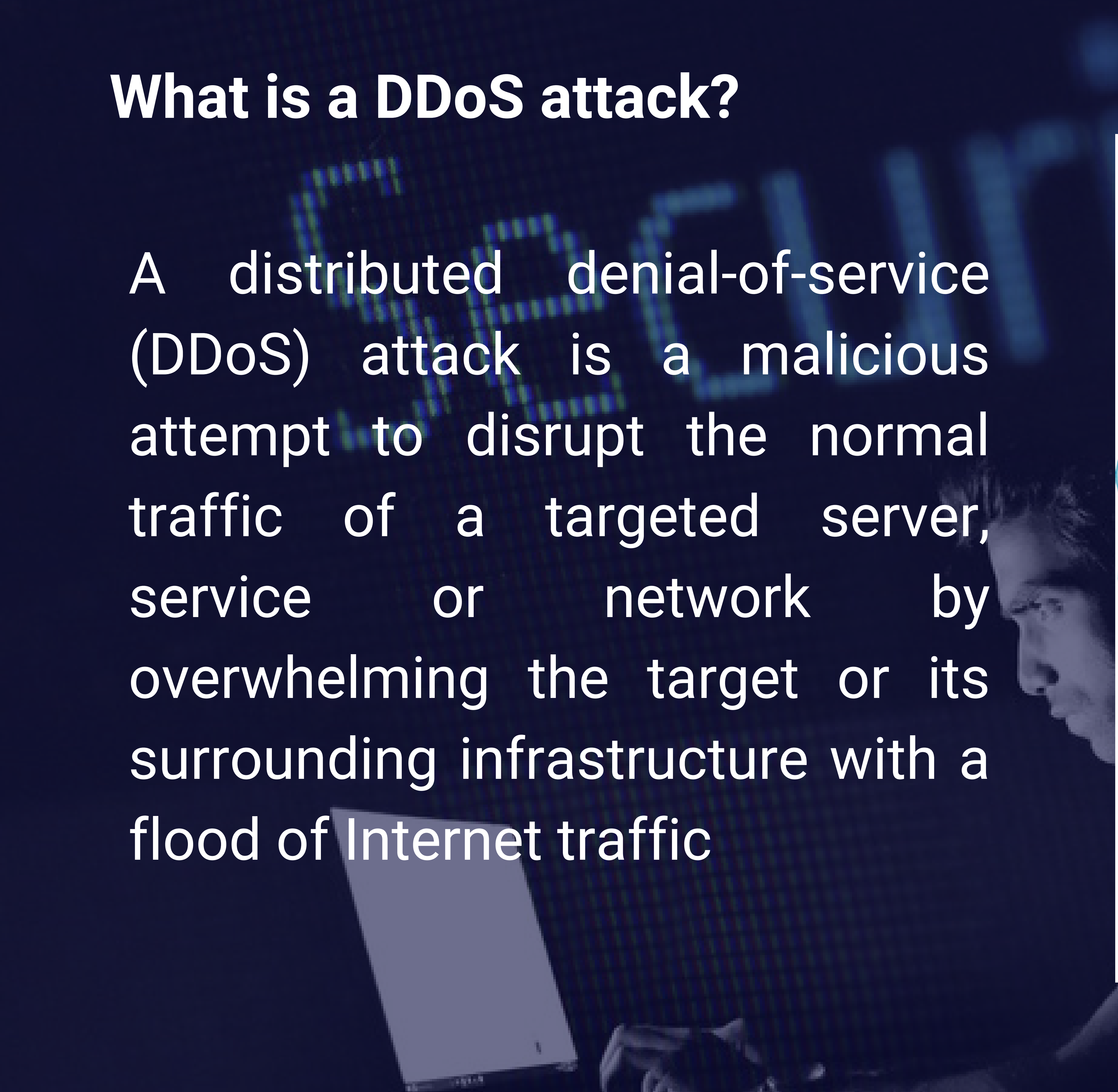
ABHIRAM B S
1BG21CS001

SUMANTH B S
1BG21CS017

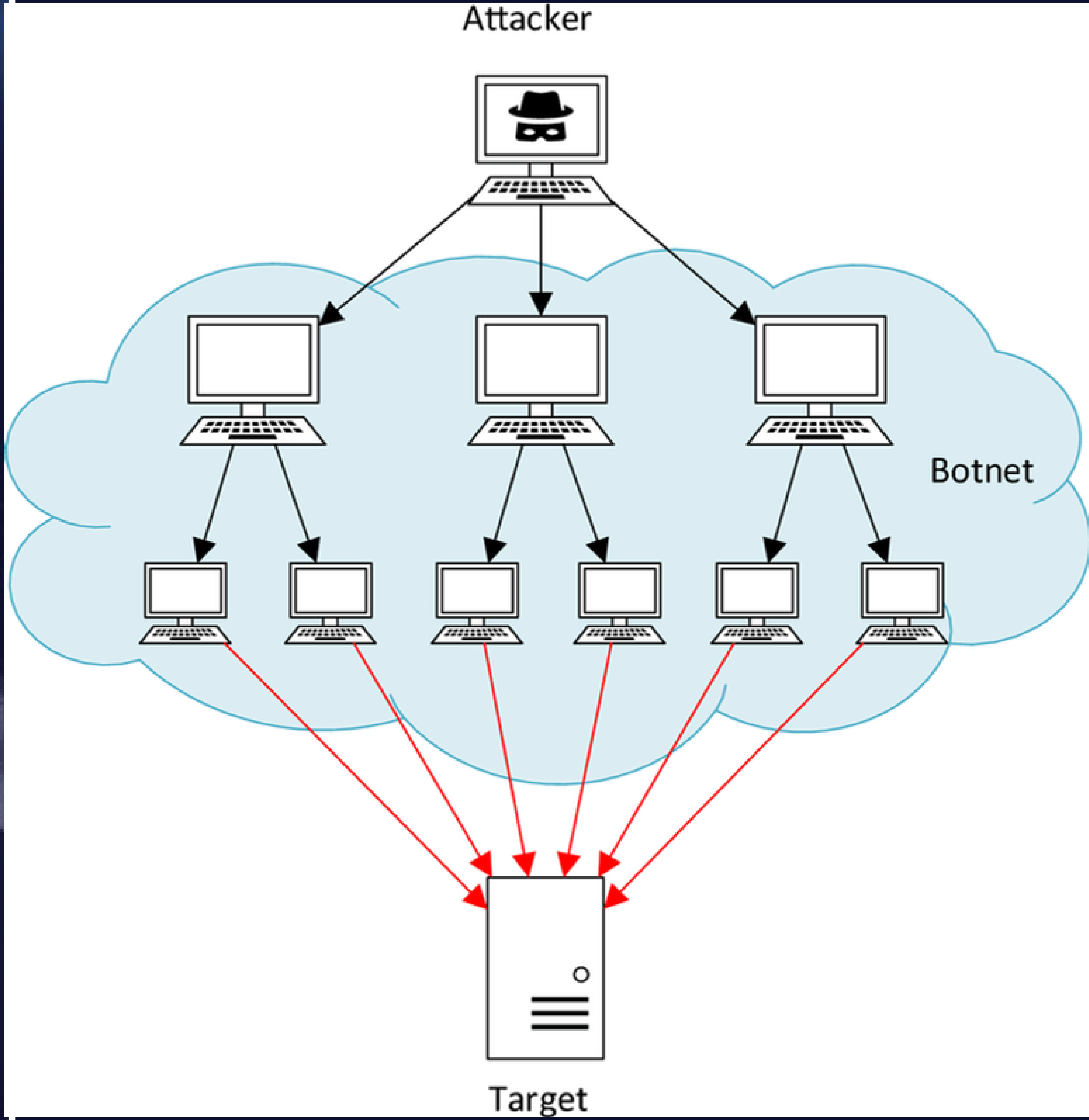
KUSHAL R
1BG21CS044

GUIDE: Prof.Pallavi C.V (Assistant Professor , DEPT:CSE)

What is a DDoS attack?



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



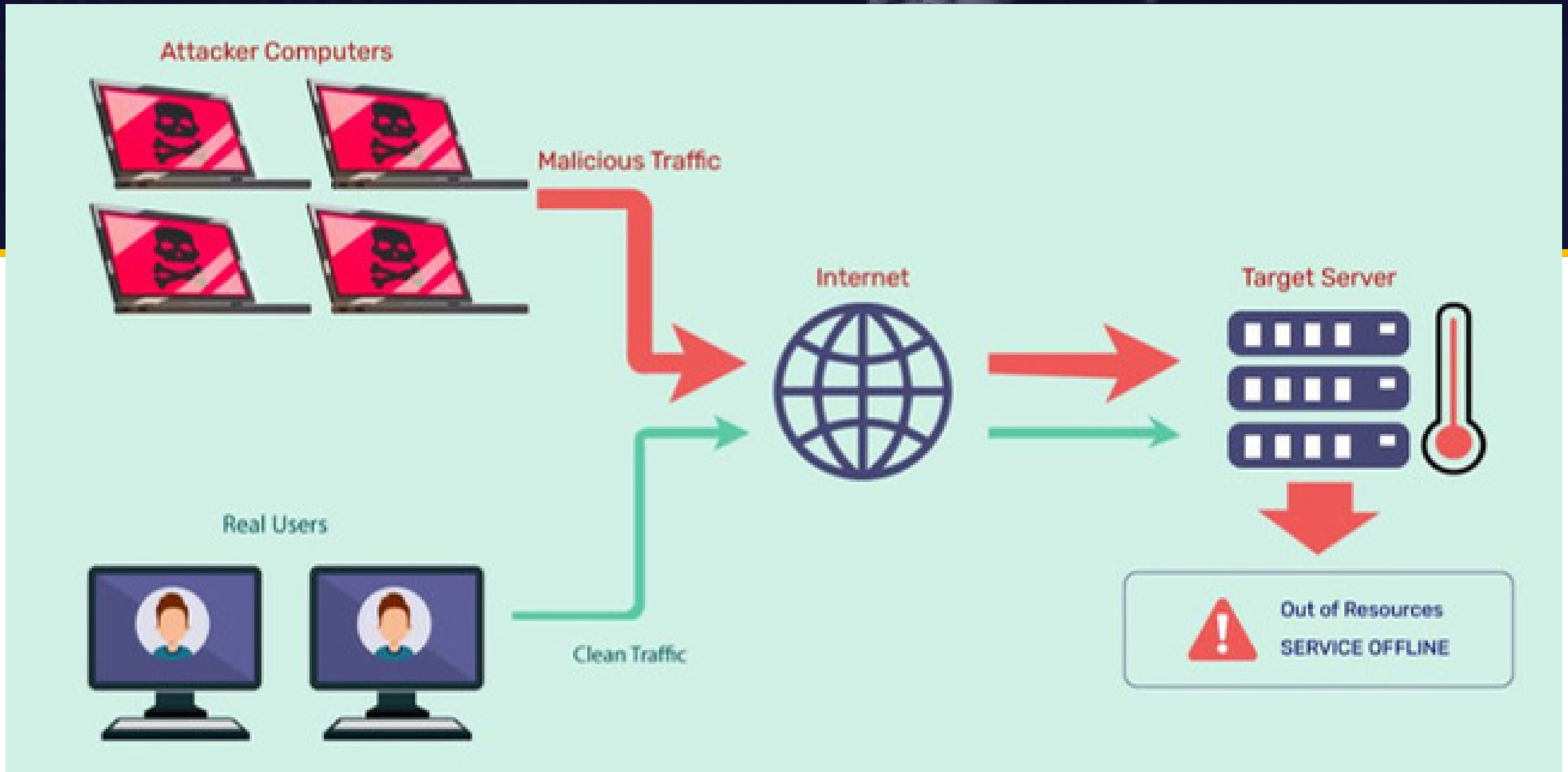
PROBLEM STATEMENT

Detecting and mitigating Distributed Denial of Service (DDoS) attacks is a critical challenge in network security.

Existing rule-based and signature-based approaches are inadequate due to their inability to adapt to evolving attack patterns, high false positive rates, and lack of real-time capabilities.

Manual intervention is often required, leading to delayed detection and response.

To address these limitations, there is a need to develop an effective DDoS detection system using machine learning algorithms.



OBJECTIVES

- Develop a robust and accurate DDoS detection model: The primary objective is to create a machine learning model that can effectively differentiate between normal network traffic and DDoS attack traffic.

- Minimize false positive rates: The objective is to optimize the machine learning model to reduce false positives and improve the accuracy of distinguishing between legitimate traffic and DDoS attacks.

Literature Survey

Author	Title	Methodology Used	Reference
C M Nalayinil, Dr. Jeevaa Katiravan	Detection of DDoS Attack using Machine Learning Algorithms	DDoS attacks are common threats where malicious users flood websites or servers with unwanted data, causing delays for legitimate users. Using eight supervised machine learning algorithms and the CIC-IDS2017 dataset, the study identifies Random Forest as the best model with 99.885% accuracy, 99.88% precision, 100% recall, and a 0.05% false alarm rate. Further research will concentrate on feature optimization and proprietary datasets for validation.	Journal of Emerging Technologies and Innovative Research (JETIR) , 2022 JETIR July 2022, Volume 9, Issue 7, www.jetir.org (ISSN-2349-5162)
Kimmi Kumari , M. Mrunalini	Detecting Denial of Service attacks using machine learning algorithms	DDoS attacks are a serious threat, impacting server resources and legitimate users. This study proposes a mathematical model using Logistic Regression and Naive Bayes for DDoS detection. Results show Logistic Regression's superiority in accuracy, MAE, and recall for attacks. Emphasizing multiple metrics for evaluation, future research may optimize and explore other techniques to improve DDoS detection.	Journal of Big Data (2022) 9:56 https://doi.org/10.1186/s40537-022-00616-0.

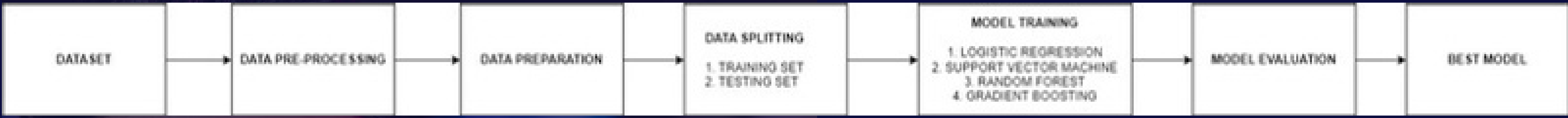
Literature Survey

Author	Title	Methodology Used	Reference
Jiangtao Pei, Yunli Chen, Wei Ji	A DDoS Attack Detection Method Based on Machine Learning	The study developed a method for detecting DDoS attacks using machine learning. It involved extracting characteristics from attack traffic and training a random forest algorithm for detection. The model's accuracy was evaluated through tests using a combination of attack and normal traffic data.	IOP Conf. Series: Journal of Physics: Conf. Series 1237 (2019) 032040
Muhammad Waqas Nadeem, Hock Guan Goh , Vasaki Ponnusamy and Yichiet Aun	DDoS Detection in SDN using Machine Learning Techniques	The research aims to enhance DDoS detection in Software-Defined Networking (SDN) environments using machine learning techniques. By leveraging ML algorithms, the study seeks to identify and mitigate DDoS attacks more effectively, enabling SDN controllers to dynamically adapt and protect the network in real-time. This approach offers proactive defense mechanisms against DDoS threats, ensuring the stability and availability of SDN-based infrastructures.	Computers, Materials & Continua DOI:10.32604/cmc.2022.021669

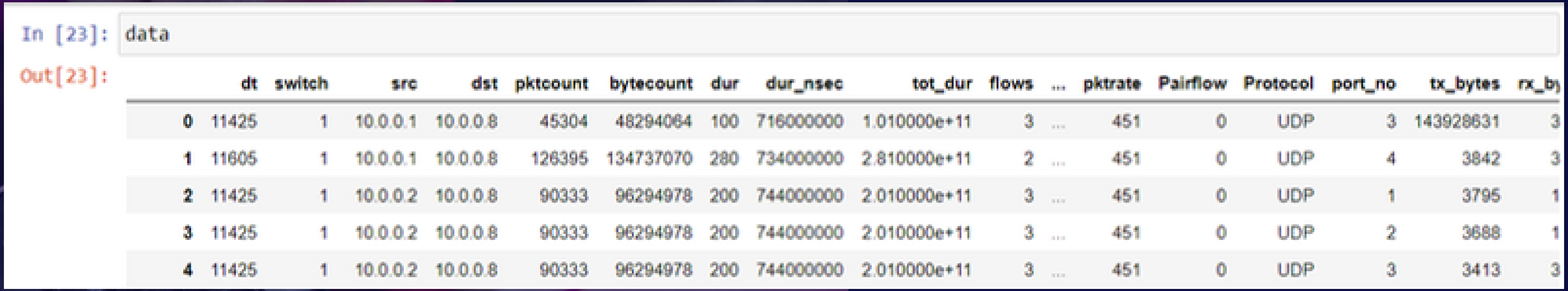
Literature Survey

Author	Title	Methodology Used	Reference
Deepak Kumar , R.K.Pateriya, Rajeev Kumar Gupta, Vasudev Dehalwar, Ashutosh Sharma	DDoS Detection using Deep Learning	DDoS detection using deep learning involves leveraging neural network architectures to automatically learn complex patterns and features indicative of DDoS attacks. By training on large-scale network traffic data, deep learning models can efficiently detect anomalous behavior and distinguish legitimate traffic from malicious traffic, leading to more accurate and robust DDoS detection systems. This approach offers the potential for real-time, proactive defense against evolving DDoS threats in diverse network environments.	Procedia Computer Science 218 (2023) 2420–2429

Methodology



Data visualization is the representation of data through use of common graphics, such as charts, plots, infographics, and even animations. These visual displays of information communicate complex data relationships and data-driven insights in a way that is easy to understand.



```
In [23]: data

Out[23]:
      dt  switch       src       dst  pktcount  bytecount  dur   dur_nsec       tot_dur  flows  ...  pktrate  Pairflow  Protocol  port_no   tx_bytes  rx_by
0  11425       1  10.0.0.1  10.0.0.8     45304   48294064  100  716000000  1.010000e+11      3  ...      451         0       UDP        3  143928631      3
1  11605       1  10.0.0.1  10.0.0.8    126395  134737070  280  734000000  2.810000e+11      2  ...      451         0       UDP        4       3842      3
2  11425       1  10.0.0.2  10.0.0.8     90333   96294978  200  744000000  2.010000e+11      3  ...      451         0       UDP        1       3795      1
3  11425       1  10.0.0.2  10.0.0.8     90333   96294978  200  744000000  2.010000e+11      3  ...      451         0       UDP        2       3688      1
4  11425       1  10.0.0.2  10.0.0.8     90333   96294978  200  744000000  2.010000e+11      3  ...      451         0       UDP        3       3413      3
```

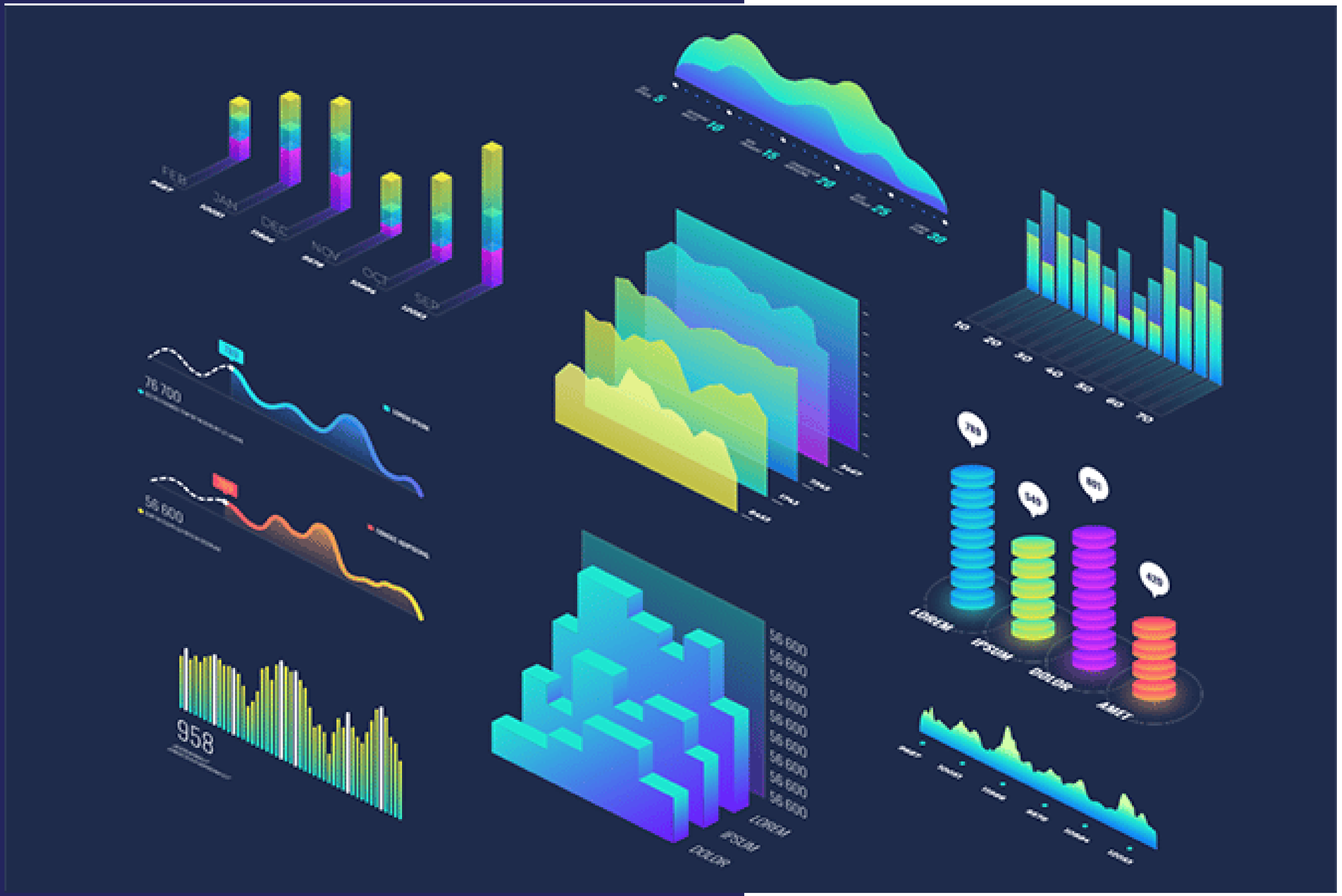
Techonologies Used:

Tools Used:

- Python 3.9
- Jupyter Notebook
- Kali Linux
- WireShark

Libraries Used:

- Pandas
- Numpy
- Matplotlib
- Seaborn
- SkLearn
- GoldenEye

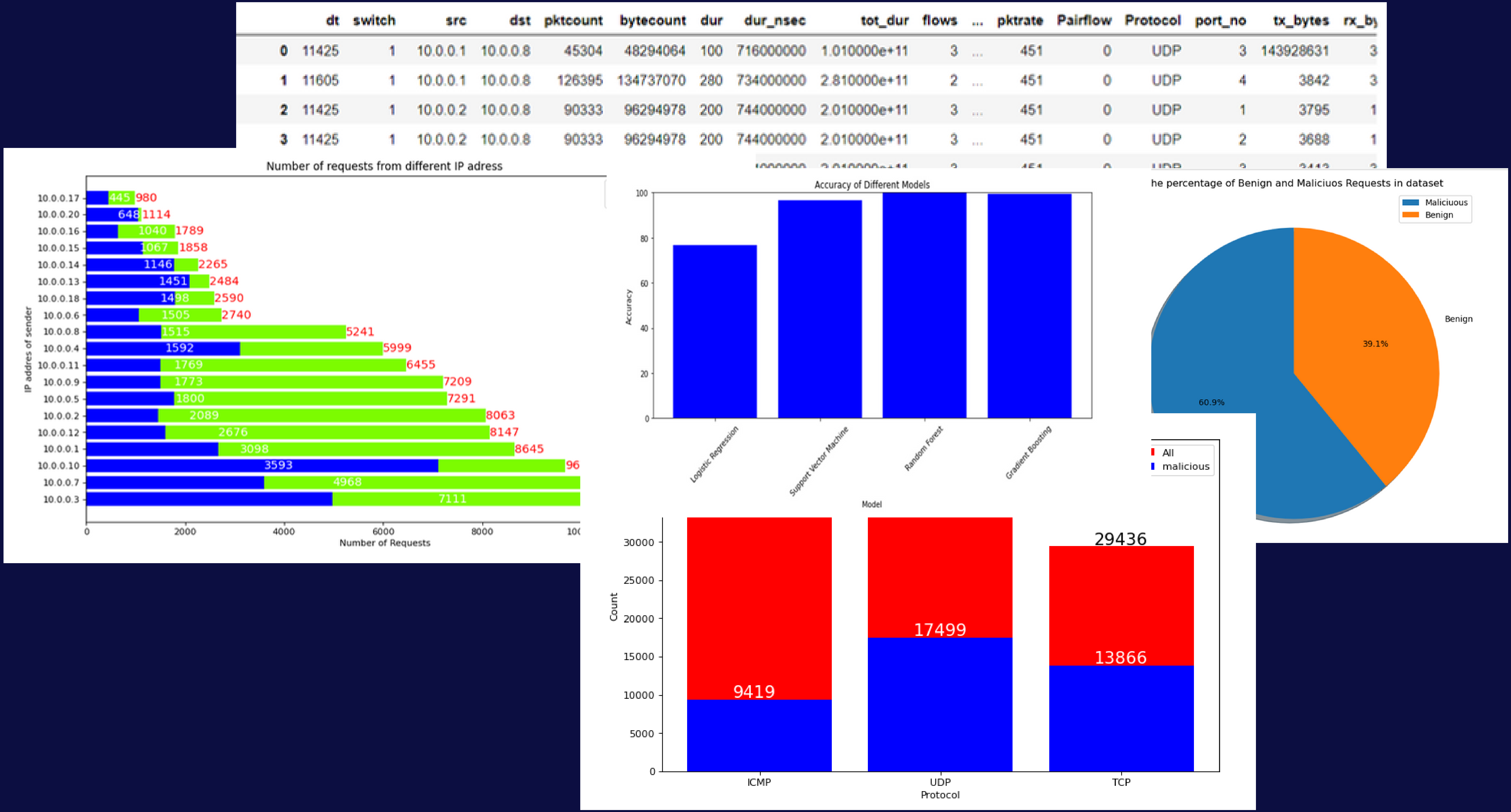


Modules implemented

Basic Data Visualization to gain the insight of the dataset. The information gathered are:

- Various attributes in the dataset
- Separation of Numeric and Object Features
- Source and Destination IP address
- percentage of Benign and Maliciuos Requests in dataset
- Implementations of Different ML Algorithms
- Selection of the Best Algorithm

Output and Demo



	dt	switch	src	dst	pktcount	bytecount	dur	dur_nsec	tot_dur	flows	...	pktrate	Pairflow	Protocol	port_no	tx_bytes	rx_by
0	11425	1	10.0.0.1	10.0.0.8	45304	48294064	100	716000000	1.010000e+11	3	...	451	0	UDP	3	143928631	3
1	11605	1	10.0.0.1	10.0.0.8	126395	134737070	280	734000000	2.810000e+11	2	...	451	0	UDP	4	3842	3
2	11425	1	10.0.0.2	10.0.0.8	90333	96294978	200	744000000	2.010000e+11	3	...	451	0	UDP	1	3795	1
3	11425	1	10.0.0.2	10.0.0.8	90333	96294978	200	744000000	2.010000e+11	3	...	451	0	UDP	2	3688	1

Conclusion

- completed data analysis and visualization, gaining valuable insights into the dataset.
- exploratory analysis helped us understand the characteristics of normal and potentially malicious traffic.
- The evaluation through various ML algorithms and selection of the model with highest accuracy.

References

- *C M Nalayinil, Dr. Jeevaa Katiravan , "Detection of DDoS Attack using Machine Learning Algorithms" , Journal of Emerging Technologies and Innovative Research (JETIR) , 2022 JETIR July 2022, Volume 9, Issue 7, www.jetir.org (ISSN-2349-5162)*
- *Kimmi Kumari , M. Mrunalini , "Detecting Denial of Service attacks using machine learning algorithms" , Journal of Big Data (2022) 9:56 https://doi.org/10.1186/s40537-022-00616-0.*
- *Jiangtao Pei, Yunli Chen, Wei Ji , "A DDoS Attack Detection Method Based on Machine Learning" , IOP Conf. Series: Journal of Physics: Conf. Series 1237 (2019) 032040*
- *Muhammad Waqas Nadeem, Hock Guan Goh , Vasaki Ponnusamy and Yichiet Aun , "DDoS Detection in SDN using Machine Learning Techniques" ,Computers, Materials & Continua DOI:10.32604/cmc.2022.021669*
- *Deepak Kumar , R.K.Pateriya, Rajeev Kumar Gupta, Vasudev Dehalwar, Ashutosh Sharma , "DDoS Detection using Deep Learning" , Procedia Computer Science 218 (2023) 2420–2429*
- *https://www.kaggle.com/code/aikenkazin/ddos-attack-detection-classification/input*
- *https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/#:~:text=your%20personal%20data.-,What%20is%20a%20DDoS%20attack%3F,a%20flood%20of%20Internet%20traffic.*
- *https://www.vmware.com/in/topics/glossary/content/software-defined-networking.html#:~:text=Software%2DDefined%20Networking%20(SDN),direct%20traffic%20on%20a%20network.*

Thank you!