Machine Learning-Driven Network Security: IoT DDoS Attack Detection

GROUP 4
Aradhya Alva Rathnakar
Bhavan Kumar Basavaraju
Mahamaya Panda
Namratha Sampath Kumar
Shashi Kumar Kadari Mallikarjuna

Introduction

01

IoT enables easy access to cloud services but faces severe DDoS threats.

02

DDoS attacks disrupt IoT services by flooding networks with compromised devices.

IoT Expansion & Vulnerability: IoT expansion requires robust security against evolving DDoS threats

Evolving DDoS Threats: Traditional measures fall short, necessitating adaptive machine learning for dynamic threat detection.

Critical Data Security: With sensitive data at stake, ML ensures data integrity and user trust.

Objective

Detect	Detect DDoS attacks in IoT environments
Utilize	Utilize innovative machine learning, with a focus on behavior analysis
Mitigate	Mitigate malicious activities causing outages and data breaches

Literature Survey

References	About the Dataset	Models Used	Results
Shahid, M., Blanc, G., Jiang, X., & Débar, H. (2018). IoT Devices Recognition Through Network Traffic Analysis. 2018 IEEE International Conference on Big Data (Big Data). https://doi.org/10.1109/bigdata.2018.8622243	A small smart home network is built to generate network traffic using four IOT devices : a Nest security camera, a D-Link motion sensor, a TP-Link smart bulb and a TP-Link smart plug. The network traffic is collected thanks to a Raspberry Pi placed between the wireless access point and the Internet	Six different classification algorithms are tested: Random Forest, Decision Tree, SVM (with rbf kernel), k-Nearest Neighbors, Artificial Neural Network (ANN) and Gaussian Naïve Bayes.	An overall accuracy of 99.9% has been achieved by the Random Forest classifier.
Patel, S., Gupta, A., Nikhil, Kumari, S., Singh, M., & Sharma, V. (2018). Network traffic classification analysis using machine learning algorithms. 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN). https://doi.org/10.1109/icacccn.2018.8748290	Wire Shark tool was used for capturing the network packet of real time data of Internet surfing for duration of 1 hour and produce around 85000 entries.	K nearest neighbours, Naïve Bayes Algorithm, Decision Tree Algorithm and Support Vector Machine.	The results show that KNN is most robust among the algorithms: NB, DT, and SVM while having highest mean for accuracy of 92.4214% for K = 11
Liang, X., & Kim, Y. (2021). A Survey on Security Attacks and Solutions in the IoT Network. 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC). https://doi.org/10.1109/ccwc51732.2021.9376174	Data collected from IOT devices (Edge Computing)	SVM, Random Forest and Logistic Regression.	SVM performed the best with an accuracy of 95.24% at detecting DDoS attacks
Neto, E. C. P., Dadkhah, S., Ferreira, R., Zohourian, A., Lu, R., & Ghorbani, A. A. (2023). CICIOT2023: A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment. *Sensors*, *23*(13), 5941. https://doi.org/10.3390/s23135941	The IoT topology was deployed to produce the CICIoT2023 dataset and comprises 105 IoT devices. A total of 67 IoT devices were directly involved in the attacks and other 38 Zigbee and Z-Wave devices were connected to five hubs to mimic a real-world deployment of IoT products and services in a smart home environment	Logistic Regression, Perceptron , Adaboost, Random Forest, and Deep Neural Network	Both Random Forest and Deep Neural Network are able to maintain high accuracy and F-1 score. These methods also present a decrease in performance but are capable of achieving F1 scores of 70%.

CRISP-DM Methodology

Business Understanding
- Project Requirements
  - Understand the Source IoT data
- Identify the domain and formulate the problem statement

Data Understanding
- Discovery of datasets for IoT DDoS attacks
- Conduct EDA

Data Preparation
- Data Cleaning
- Data Transformation
- Split of Data into Train (80%) and Test (20%)

Modeling
- Develop Models
  - KNN
  - RF
  - SVM
- Implement Ensemble technique
  - RF + KNN
  - KNN + SVM
  - RF + SVM

Evaluation
- Model Validation
- Evaluation Metrics
  - F1 Score
  - Accuracy
  - Confusion Matrix

Deployment
- Deploy the model for final usage in Streamlit

Data Source

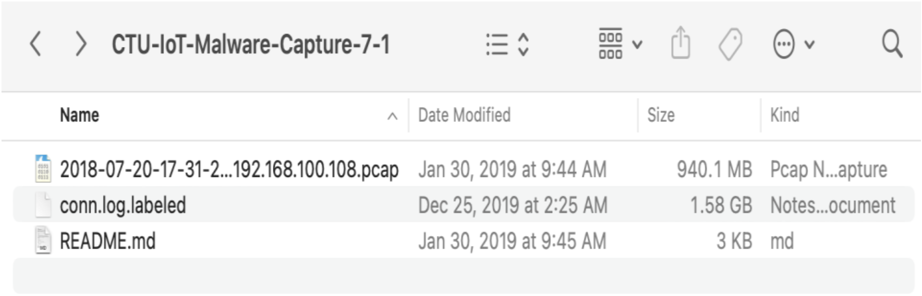
Data is sourced from Aposemat IoT-23 which was created as part of Avast AIC laboratory ranging from 2018-2019 and was published in the year 2020

“Sebastian Garcia, Agustin Parmisano, & Maria Jose Erquiaga. (2020). IoT-23: A labeled dataset with malicious and benign IoT network traffic (Version 1.0.0) [Data set]. Zenodo. http://doi.org/10.5281/zenodo.4743746”

Data Collection

Data is retrieved from different file formats as follows:

- README.md - contains info about captures and associated malwares.
- .pcap - original file that has network traffic captures
- conn.log.labeled - .pcap file is retrieved using Zeek network analyser with proper labelling along with some additional info



CTU-IoT-Malware-Capture-7-1 (Linux.Mirai)

LABELS DISTRIBUTION

Label	Flows
Benign	75,955
C&C-HeartBeat	5,778
DDoS	39,584
Okiru	11,333,397

LINK TO THIS DATASET FILES:

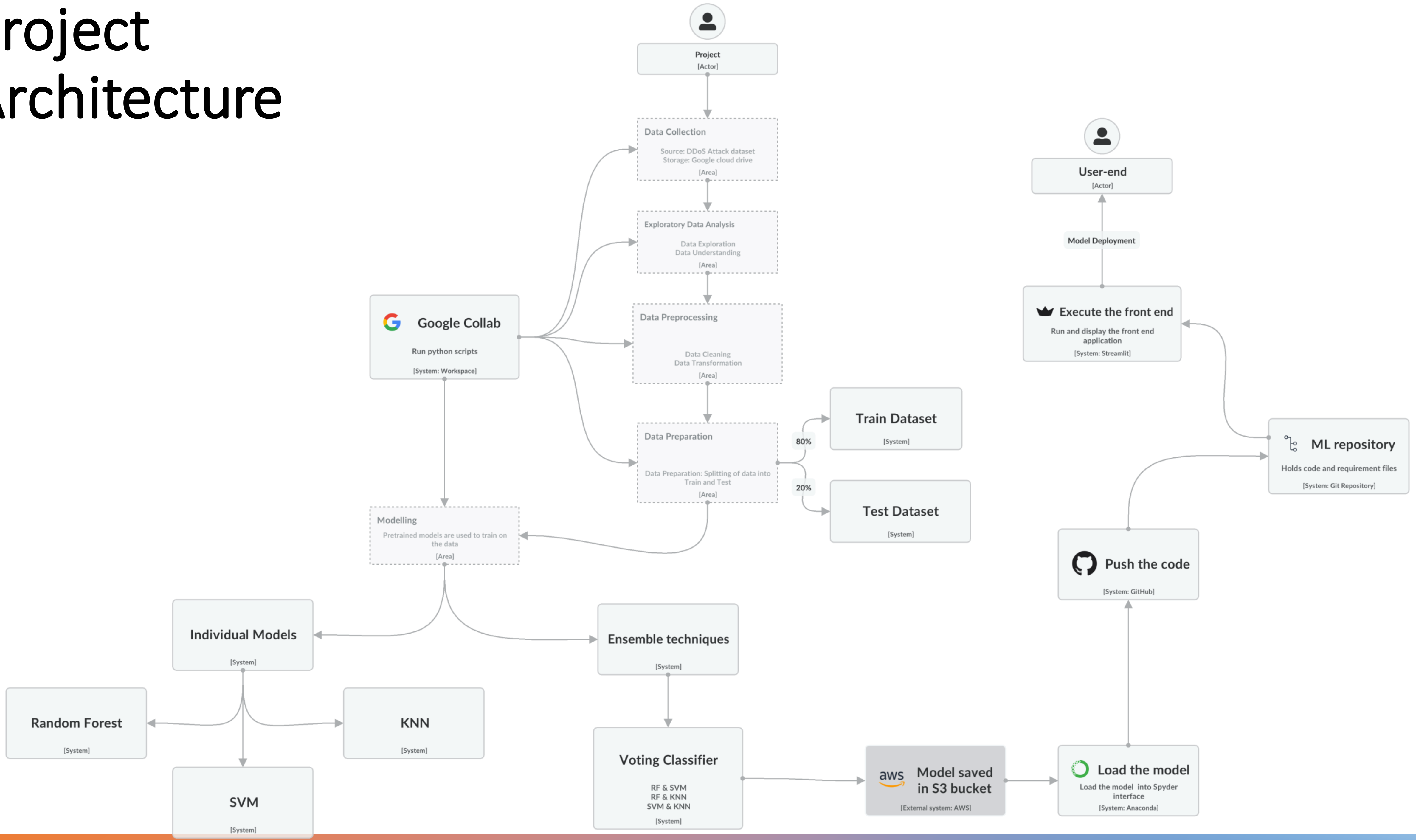
https://mcfp.felk.cvut.cz/publicDatasets/IoT-23-Dataset/IndividualScenarios/CTU-IoT-Malware-Capture-7-1/

About the dataset

Aposemat IoT-23

- A unique dataset capturing IoT network traffic.
- 20 malware captures on IoT devices and 3 benign IoT devices.
- Real network behaviour for research and machine learning.
- Labels provided for analysis, including attack, C&C, DDoS, and more.
- A valuable resource for IoT security and malware research.

Project Architecture



Data Process Flow

Source IoT Data

- CSV format

EDA

- Null checks
- Statistical distribution
- Correlation of columns

Data Cleansing

- Drop unwanted columns
- Rename columns
- Handle Missing values through mean imputation
- Replace '-' with nulls
- Drop duplicate records

Data Transformation

- Label encoding to handle categorical features
- Standardize the numerical features
- Bin the different attacks into DDoS and Non- DDoS
- Apply RandomOverSampler to the minority class
- Data Regularization

Data Preparation

- 80% training dataset
- 20% testing dataset

Source IoT Data

Download the full IoT-23 dataset (21 GB) here:

- https://mcfp.felk.cvut.cz/publicDatasets/IoT-23-Dataset/iot_23_datasets_full.tar.gz

Download a lighter version containing only the labeled flows without the pcaps files (8.8 GB) here:

- https://mcfp.felk.cvut.cz/publicDatasets/IoT-23-Dataset/iot_23_datasets_small.tar.gz

Download the design of how the **labels** were assigned from this spreadsheet

- https://docs.google.com/spreadsheets/d/1HRqgKJpoXoSUIfW3rCQKoD_LnSCJ1k-k61PndJXWq_0/edit#gid=0

Exploratory Data Analysis

- Available columns: 21
- Datatypes: object (14 columns), float64 (7 columns)
- Total records: 11,448,425

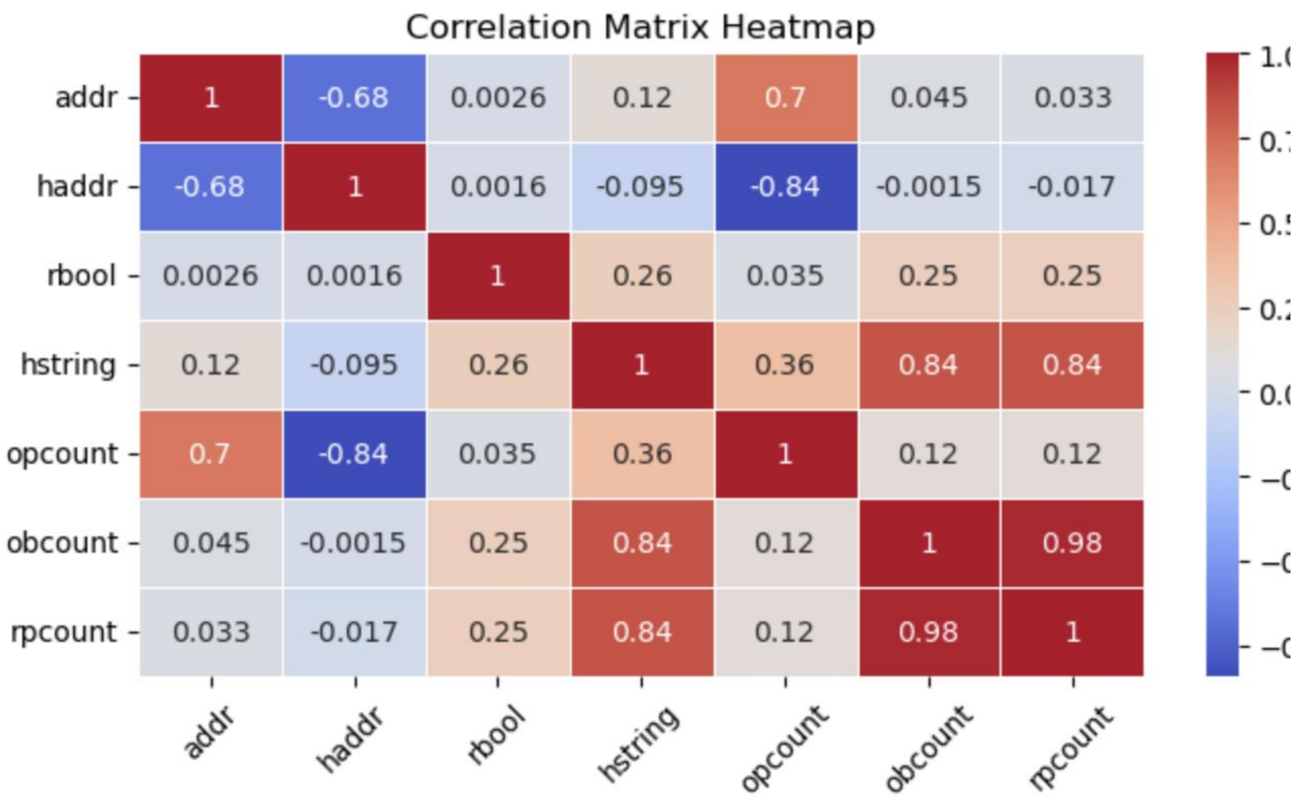
#	Column	Dtype
---	------	-----
0	#types	object
1	t	object
2	uidstring	object
3	addr	float64
4	port	object
5	haddr	float64
6	pport	object
7	enum	object
8	sstring	object
9	interval	object
10	bcount	object
11	rcount	object
12	connstring	object
13	obool	object
14	rbool	float64
15	mbcount	object
16	hstring	float64
17	opcount	float64
18	obcount	float64

Exploratory Data Analysis

- #types has no nulls.
- T has 1 null value.
- The rest of the columns have 2 null values.

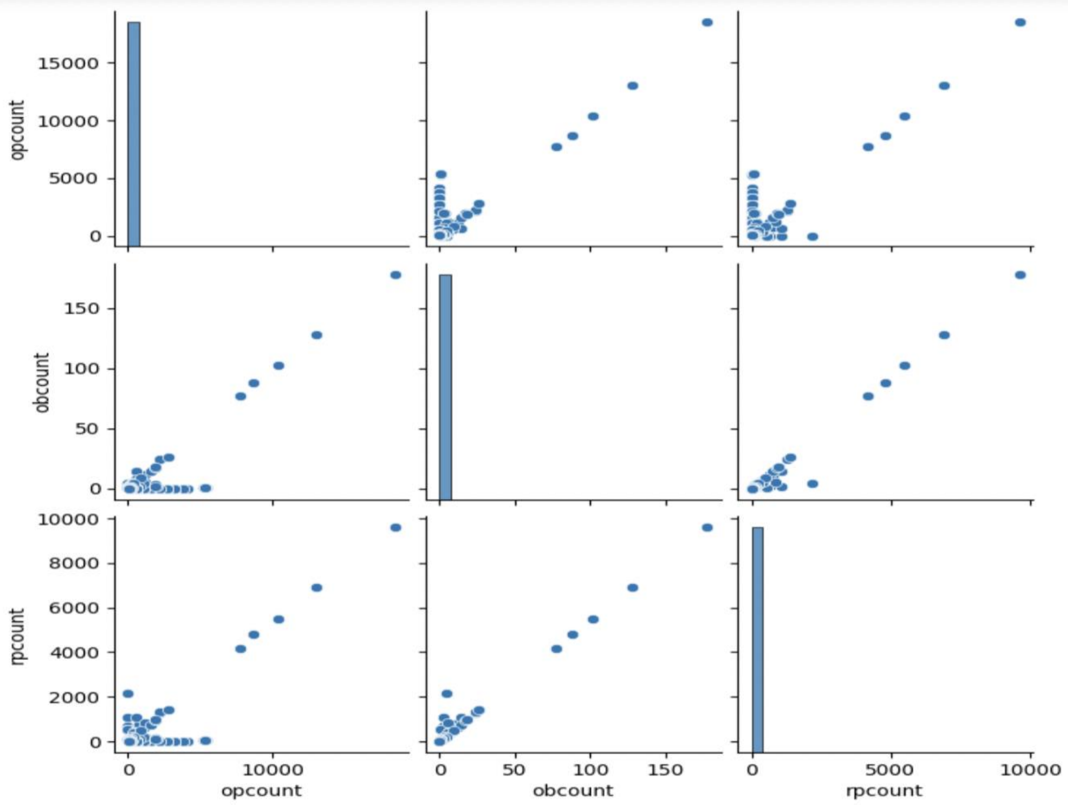
```
#types        0
t             1
uidstring     2
addr          2
port          2
haddr         2
pport         2
enum          2
sstring       2
interval      2
bcount        2
rcount        2
connstring    2
obool         2
rbool         2
mbcount       2
hstring       2
opcount       2
obcount       2
rpcount       2
ipbcount      2
dtype: int64
```

Exploratory Data Analysis



- Correlation matrix analysis reveals relationships among attributes related to DDoS attacks.
- 'obcount' and 'rp count' show the highest correlation in the dataset.
- Understanding this correlation is crucial for shaping effective feature engineering in attack detection.

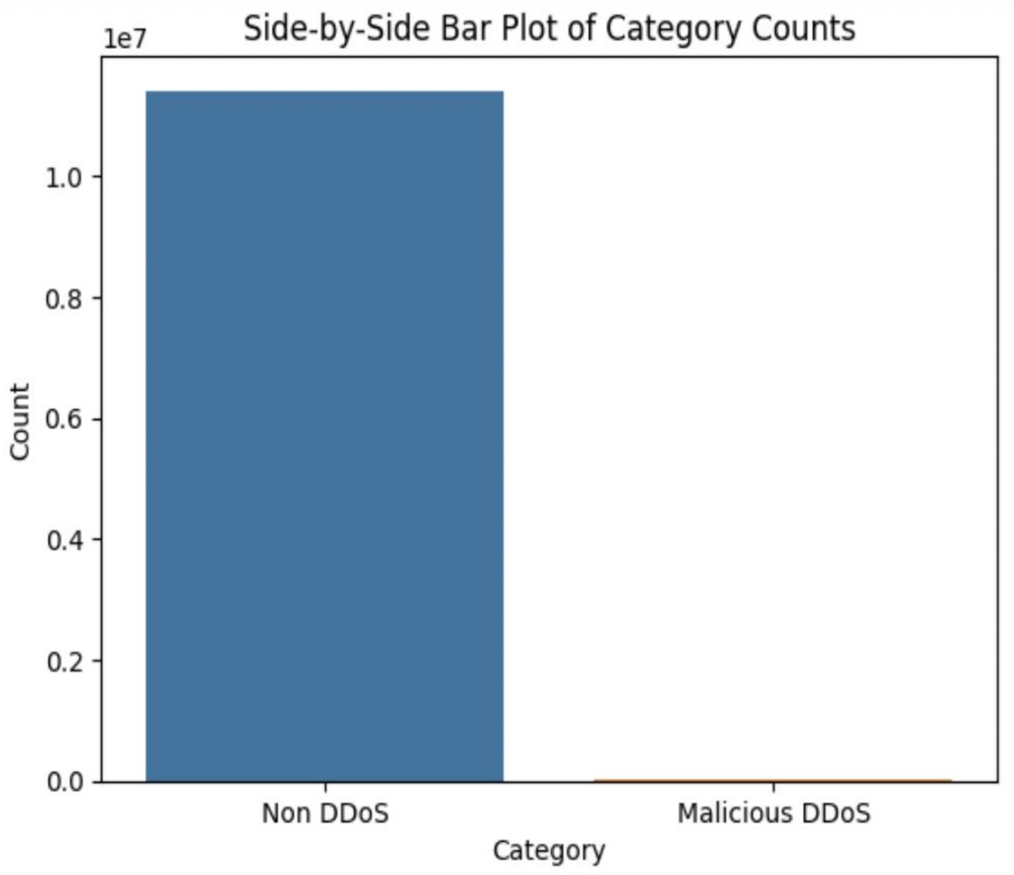
Exploratory Data Analysis

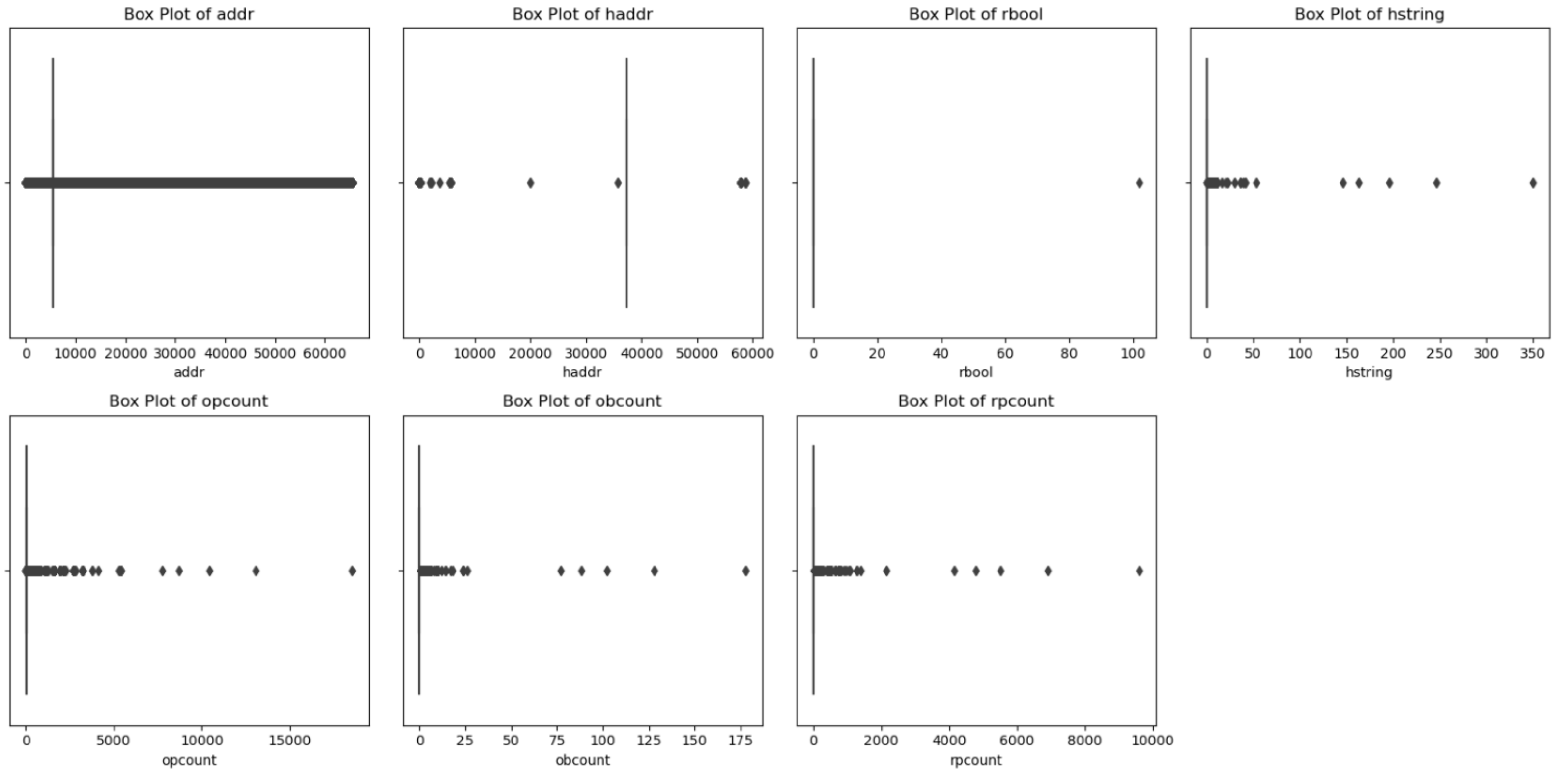


- Pair plot visualization offers insights into relationships and distributions in the dataset.
- Useful for identifying potential correlations and patterns related to DDoS attack activity.

Exploratory Data Analysis

- Bar plot categorizes data into 'Non DDoS' and 'Malicious DDoS.'
- 'Non DDoS' count is 11,408,840, and 'Malicious DDoS' count is 39,584, indicating class imbalance.
- Distribution is crucial for building effective DDoS detection models.





- Statistical distribution of values.
- For hstring, opcount, obcount, and rpcount, the values are closer to the median.
- The values for addr are spread out evenly since it is a unique identifier
- The values for haddr are spread out evenly as well.

Exploratory Data Analysis

Data Cleaning

	#types	t	uidstring	addr	port	haddr	pport	enum	sstring	interval	...	rcount	connstring	obool	rbool	mbcount	hstring	opcount	obcount	rpcount	ipbcount
0	1532100786.102371	CWeq2B3YXkMYfJ5sl	192.168.100.108	5353.0	224.0.0.251	5353.0	udp	dns	4.133830	1193	...	S0	-	-	0.0	D	11.0	1501.0	0.0	0.0	(empty) Benign -
1	1532100812.196921	CYLFGG1WiaMTVZbVed	192.168.100.108	54360.0	192.168.100.1	53.0	udp	dns	0.000997	78	...	SF	-	-	0.0	Dd	2.0	134.0	2.0	198.0	(empty) Benign -
2	1532100813.201597	CXLNuE10OdgwToBlb8	192.168.100.108	53971.0	192.168.100.1	53.0	udp	dns	0.054470	78	...	SF	-	-	0.0	Dd	2.0	134.0	2.0	310.0	(empty) Benign -
3	1532100814.272486	COdAkSYAcGOu6J139	192.168.100.108	57415.0	192.168.100.1	53.0	udp	dns	0.053221	78	...	SF	-	-	0.0	Dd	2.0	134.0	2.0	253.0	(empty) Benign -
4	1532100814.328455	CrDWAb2lPhhFQIN75e	192.168.100.108	34266.0	192.168.100.1	53.0	udp	dns	0.031732	78	...	SF	-	-	0.0	Dd	2.0	134.0	2.0	253.0	(empty) Benign -
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...
11448421	1532187029.115683	CK0ALv1sLwqLSzihlj	212.144.235.74	3.0	192.168.100.108	1.0	icmp	-	-	-	...	OTH	-	-	0.0	-	1.0	68.0	0.0	0.0	(empty) Benign -
11448422	1532186994.959568	CcmYQw1uthYpacXVMI	193.136.134.150	3.0	192.168.100.108	1.0	icmp	-	35.342305	80	...	OTH	-	-	0.0	-	2.0	136.0	0.0	0.0	(empty) Benign -
11448423	1532187057.469573	CPzoom3ZYNkUdHfRJc	154.196.138.6	3.0	192.168.100.108	10.0	icmp	-	-	-	...	OTH	-	-	0.0	-	1.0	68.0	0.0	0.0	(empty) Benign -
11448424	1532187066.809124	CgmRAT27X32PN3he8l	154.202.131.93	3.0	192.168.100.108	10.0	icmp	-	-	-	...	OTH	-	-	0.0	-	1.0	68.0	0.0	0.0	(empty) Benign -
11448425	#close	2018-08-08-11-33-33	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	...	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN

11448426 rows × 21 columns

Before Cleaning

After Cleaning

	uid_string	id.orig_addr	id.orig_port	id.resp_haddr	missed_bytes_count	history_string	orig_pkts_count	orig_ip_bytes_count	resp_pkts_count	Category
0	192.168.100.108	5353.0	224.0.0.251	5353.0	D	11.0	1501.0	0.0	0.0	(empty) Benign -
1	192.168.100.108	54360.0	192.168.100.1	53.0	Dd	2.0	134.0	2.0	198.0	(empty) Benign -
2	192.168.100.108	53971.0	192.168.100.1	53.0	Dd	2.0	134.0	2.0	310.0	(empty) Benign -
3	192.168.100.108	57415.0	192.168.100.1	53.0	Dd	2.0	134.0	2.0	253.0	(empty) Benign -
4	192.168.100.108	34266.0	192.168.100.1	53.0	Dd	2.0	134.0	2.0	253.0	(empty) Benign -
...	...	...	...	...	...	...	...	...	...	...
11448420	2.203.14.58	3.0	192.168.100.108	13.0	NaN	1.0	56.0	0.0	0.0	(empty) Benign -
11448421	212.144.235.74	3.0	192.168.100.108	1.0	NaN	1.0	68.0	0.0	0.0	(empty) Benign -
11448422	193.136.134.150	3.0	192.168.100.108	1.0	NaN	2.0	136.0	0.0	0.0	(empty) Benign -
11448423	154.196.138.6	3.0	192.168.100.108	10.0	NaN	1.0	68.0	0.0	0.0	(empty) Benign -
11448424	154.202.131.93	3.0	192.168.100.108	10.0	NaN	1.0	68.0	0.0	0.0	(empty) Benign -

11426020 rows × 10 columns

- Null values handled through KNN imputation and deletion.
- Renaming, handling, removing, dropping data columns.

Data Transformation

Data before Label Encoding

	uid_string	id.orig_addr	id.orig_port	id.resp_haddr	missed_bytes_count	history_string	orig_pkts_count	orig_ip_bytes_count	resp_pkts_count	Category
0	192.168.100.108	5353.0	224.0.0.251	5353.0	D	11.0	1501.0	0.0	0.0	(empty) Benign -
1	192.168.100.108	54360.0	192.168.100.1	53.0	Dd	2.0	134.0	2.0	198.0	(empty) Benign -
2	192.168.100.108	53971.0	192.168.100.1	53.0	Dd	2.0	134.0	2.0	310.0	(empty) Benign -
3	192.168.100.108	57415.0	192.168.100.1	53.0	Dd	2.0	134.0	2.0	253.0	(empty) Benign -
4	192.168.100.108	34266.0	192.168.100.1	53.0	Dd	2.0	134.0	2.0	253.0	(empty) Benign -
...	...	...	...	...	...	...	...	...	...	...
11448420	2.203.14.58	3.0	192.168.100.108	13.0	NaN	1.0	56.0	0.0	0.0	(empty) Benign -
11448421	212.144.235.74	3.0	192.168.100.108	1.0	NaN	1.0	68.0	0.0	0.0	(empty) Benign -
11448422	193.136.134.150	3.0	192.168.100.108	1.0	NaN	2.0	136.0	0.0	0.0	(empty) Benign -
11448423	154.196.138.6	3.0	192.168.100.108	10.0	NaN	1.0	68.0	0.0	0.0	(empty) Benign -
11448424	154.202.131.93	3.0	192.168.100.108	10.0	NaN	1.0	68.0	0.0	0.0	(empty) Benign -

11426020 rows × 10 columns

Data after Label Encoding

	uid_string	id.orig_addr	id.orig_port	id.resp_haddr	missed_bytes_count	history_string	orig_pkts_count	orig_ip_bytes_count	resp_pkts_count	Category
0	192.168.100.108	5353.0	224.0.0.251	5353.0	1.0	11.0	1501.0	0.0	0.0	(empty) Benign -
1	192.168.100.108	54360.0	192.168.100.1	53.0	3.0	2.0	134.0	2.0	198.0	(empty) Benign -
2	192.168.100.108	53971.0	192.168.100.1	53.0	3.0	2.0	134.0	2.0	310.0	(empty) Benign -
3	192.168.100.108	57415.0	192.168.100.1	53.0	3.0	2.0	134.0	2.0	253.0	(empty) Benign -
4	192.168.100.108	34266.0	192.168.100.1	53.0	3.0	2.0	134.0	2.0	253.0	(empty) Benign -
...	...	...	...	...	...	...	...	...	...	...
11448420	2.203.14.58	3.0	192.168.100.108	13.0	NaN	1.0	56.0	0.0	0.0	(empty) Benign -
11448421	212.144.235.74	3.0	192.168.100.108	1.0	NaN	1.0	68.0	0.0	0.0	(empty) Benign -
11448422	193.136.134.150	3.0	192.168.100.108	1.0	NaN	2.0	136.0	0.0	0.0	(empty) Benign -
11448423	154.196.138.6	3.0	192.168.100.108	10.0	NaN	1.0	68.0	0.0	0.0	(empty) Benign -
11448424	154.202.131.93	3.0	192.168.100.108	10.0	NaN	1.0	68.0	0.0	0.0	(empty) Benign -

11426020 rows × 10 columns

- Utilized KNNImputer for missing values
- Imputed using five nearest neighbors.

Data Transformation

	uid_string	id.orig_addr	id.orig_port	id.resp_haddr	missed_bytes_count	history_string	orig_pkts_count	orig_ip_bytes_count	resp_pkts_count	Category
0	192.168.100.108	5353.0	224.0.0.251	5353.0	1.0	11.0	1501.0	0.0	0.0	(empty) Benign -
1	192.168.100.108	54360.0	192.168.100.1	53.0	3.0	2.0	134.0	2.0	198.0	(empty) Benign -
2	192.168.100.108	53971.0	192.168.100.1	53.0	3.0	2.0	134.0	2.0	310.0	(empty) Benign -
3	192.168.100.108	57415.0	192.168.100.1	53.0	3.0	2.0	134.0	2.0	253.0	(empty) Benign -
4	192.168.100.108	34266.0	192.168.100.1	53.0	3.0	2.0	134.0	2.0	253.0	(empty) Benign -
...	...	...	...	...	...	...	...	...	...	...
11448420	2.203.14.58	3.0	192.168.100.108	13.0	NaN	1.0	56.0	0.0	0.0	(empty) Benign -
11448421	212.144.235.74	3.0	192.168.100.108	1.0	NaN	1.0	68.0	0.0	0.0	(empty) Benign -
11448422	193.136.134.150	3.0	192.168.100.108	1.0	NaN	2.0	136.0	0.0	0.0	(empty) Benign -
11448423	154.196.138.6	3.0	192.168.100.108	10.0	NaN	1.0	68.0	0.0	0.0	(empty) Benign -
11448424	154.202.131.93	3.0	192.168.100.108	10.0	NaN	1.0	68.0	0.0	0.0	(empty) Benign -

11426020 rows × 10 columns

Data before Standarization

Data after Standarization

	uid_string	id.orig_addr	id.orig_port	id.resp_haddr	missed_bytes_count	history_string	orig_pkts_count	orig_ip_bytes_count	resp_pkts_count	Category
0	192.168.100.108	5353.0	224.0.0.251	5353.0	1.0	59.653202	22.270777	-0.016117	-0.012590	Non DDoS
1	192.168.100.108	54360.0	192.168.100.1	53.0	3.0	5.952537	1.351589	22.326843	41.504154	Non DDoS
2	192.168.100.108	53971.0	192.168.100.1	53.0	3.0	5.952537	1.351589	22.326843	64.988373	Non DDoS
3	192.168.100.108	57415.0	192.168.100.1	53.0	3.0	5.952537	1.351589	22.326843	53.036583	Non DDoS
4	192.168.100.108	34266.0	192.168.100.1	53.0	3.0	5.952537	1.351589	22.326843	53.036583	Non DDoS
...	...	...	...	...	...	...	...	...	...	...
11426015	192.168.100.108	5526.0	9.142.38.44	37215.0	29.0	-0.014204	-0.086892	-0.016117	-0.012590	Non DDoS
11426016	192.168.100.108	5526.0	77.6.97.156	37215.0	29.0	-0.014204	-0.086892	-0.016117	-0.012590	Non DDoS
11426017	192.168.100.108	5526.0	169.172.173.135	37215.0	29.0	-0.014204	-0.086892	-0.016117	-0.012590	Non DDoS
11426018	192.168.100.108	5526.0	192.188.69.18	37215.0	29.0	-0.014204	-0.086892	-0.016117	-0.012590	Non DDoS
11426019	192.168.100.108	5526.0	43.224.126.126	37215.0	29.0	-0.014204	-0.086892	-0.016117	-0.012590	Non DDoS

11403688 rows × 10 columns

- Standardized numerical columns for consistency
- Facilitates model training on common scale

Data Transformation

	uid_string	id.orig_addr	id.orig_port	id.resp_haddr	missed_bytes_count	history_string	orig_pkts_count	orig_ip_bytes_count	resp_pkts_count	Category
0	192.168.100.108	5353.0	224.0.0.251	5353.0	1.0	11.0	1501.0	0.0	0.0	(empty) Benign -
1	192.168.100.108	54360.0	192.168.100.1	53.0	3.0	2.0	134.0	2.0	198.0	(empty) Benign -
2	192.168.100.108	53971.0	192.168.100.1	53.0	3.0	2.0	134.0	2.0	310.0	(empty) Benign -
3	192.168.100.108	57415.0	192.168.100.1	53.0	3.0	2.0	134.0	2.0	253.0	(empty) Benign -
4	192.168.100.108	34266.0	192.168.100.1	53.0	3.0	2.0	134.0	2.0	253.0	(empty) Benign -

Data before binning the Category field

Data after binning

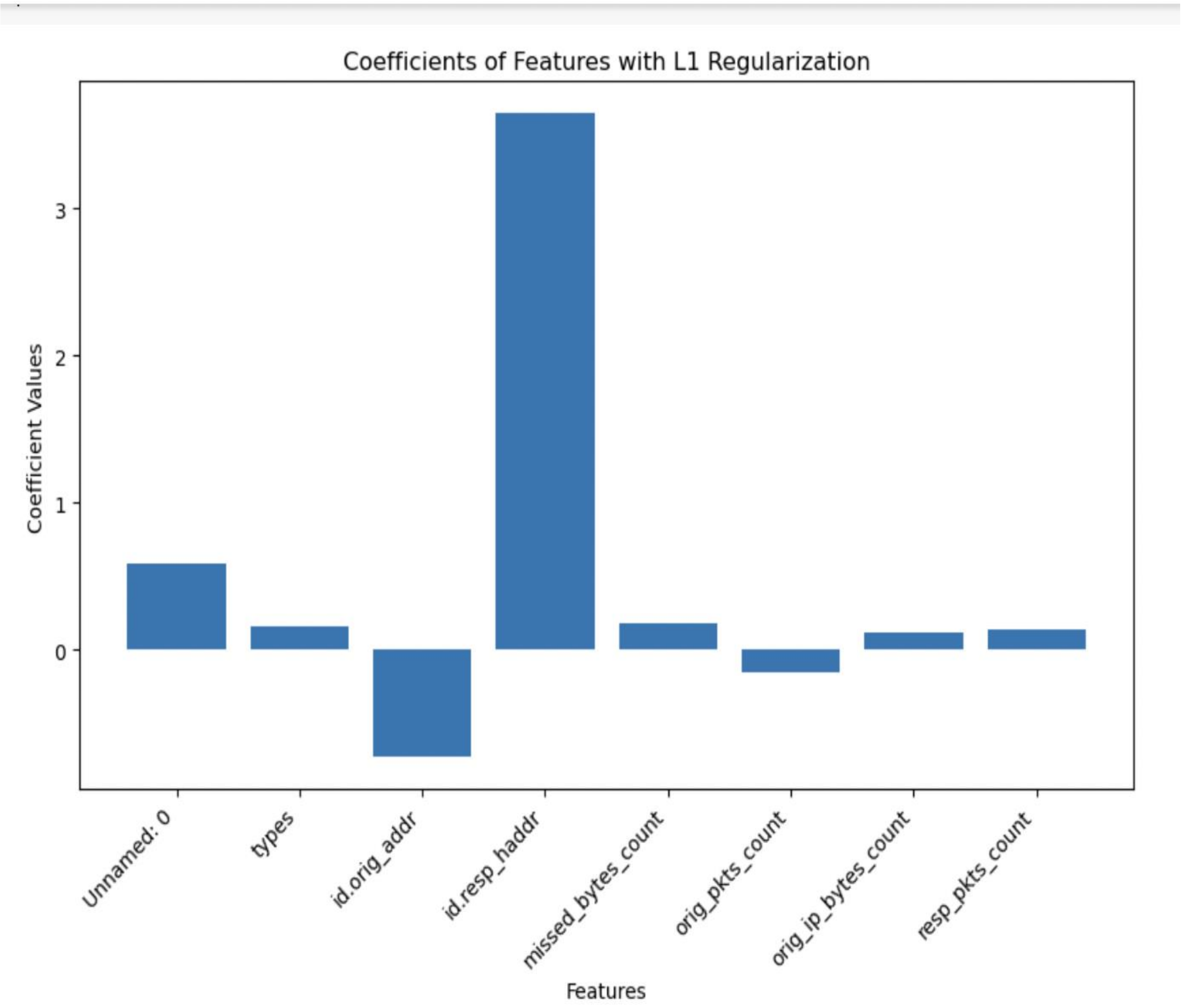
	uid_string	id.orig_addr	id.orig_port	id.resp_haddr	missed_bytes_count	history_string	orig_pkts_count	orig_ip_bytes_count	resp_pkts_count	Category
0	192.168.100.108	5353.0	224.0.0.251	5353.0	1.0	59.653202	22.270777	-0.016117	-0.012590	Non DDoS
1	192.168.100.108	54360.0	192.168.100.1	53.0	3.0	5.952537	1.351589	22.326843	41.504154	Non DDoS
2	192.168.100.108	53971.0	192.168.100.1	53.0	3.0	5.952537	1.351589	22.326843	64.988373	Non DDoS
3	192.168.100.108	57415.0	192.168.100.1	53.0	3.0	5.952537	1.351589	22.326843	53.036583	Non DDoS
4	192.168.100.108	34266.0	192.168.100.1	53.0	3.0	5.952537	1.351589	22.326843	53.036583	Non DDoS
...	...	...	...	...	...	...	...	...	...	...
11426015	192.168.100.108	5526.0	9.142.38.44	37215.0	29.0	-0.014204	-0.086892	-0.016117	-0.012590	Non DDoS
11426016	192.168.100.108	5526.0	77.6.97.156	37215.0	29.0	-0.014204	-0.086892	-0.016117	-0.012590	Non DDoS
11426017	192.168.100.108	5526.0	169.172.173.135	37215.0	29.0	-0.014204	-0.086892	-0.016117	-0.012590	Non DDoS
11426018	192.168.100.108	5526.0	192.188.69.18	37215.0	29.0	-0.014204	-0.086892	-0.016117	-0.012590	Non DDoS
11426019	192.168.100.108	5526.0	43.224.126.126	37215.0	29.0	-0.014204	-0.086892	-0.016117	-0.012590	Non DDoS

11403688 rows × 10 columns

- Binning categorizes attacks into 'DDoS' and 'Non DDoS' using a mapping dictionary for count.

Data Transformation

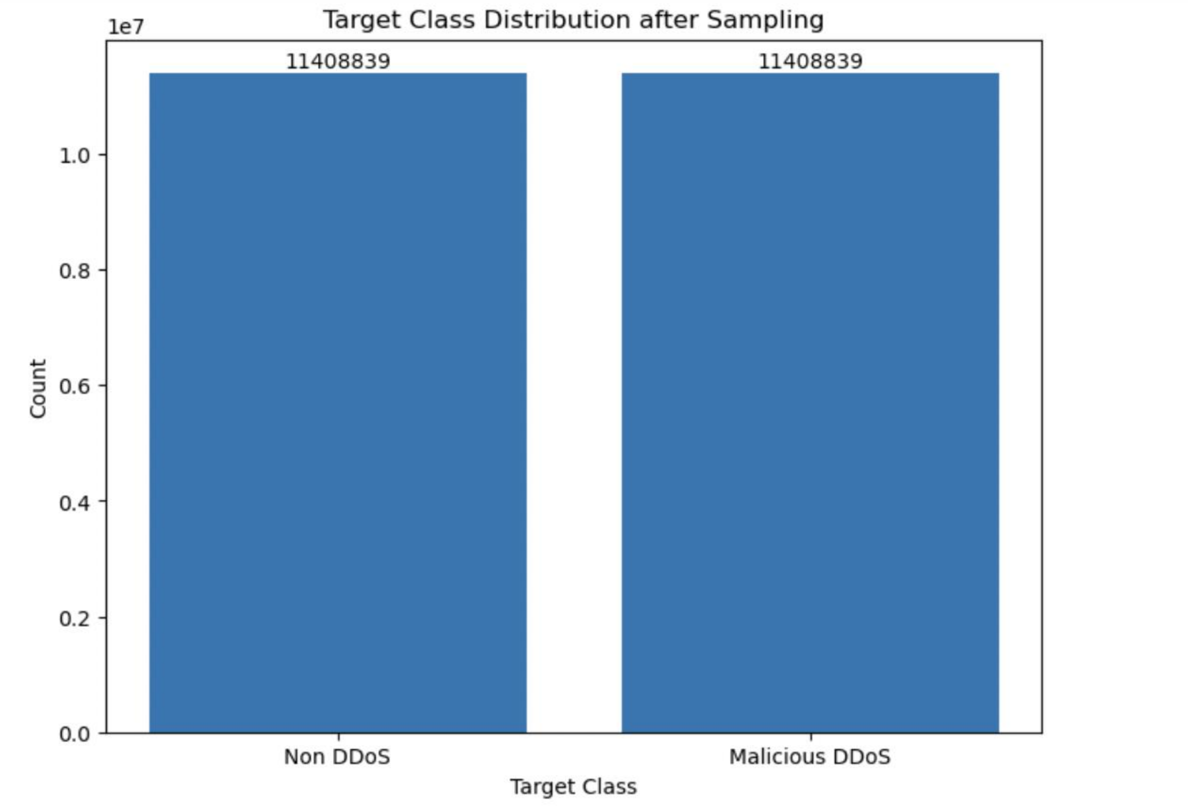
- Visualizes coefficient changes with regularization
- Coefficients show features' contribution to prediction



Data Transformation

- Addresses data imbalance using sampling
- Ensures model neutrality during training

```
Target class distribution
Category
Non DDoS           11408839
Malicious DDoS        39584
Name: count, dtype: int64
Target class distribution after Sampling
0    11408839
1    11408839
Name: count, dtype: int64
Target class(train) distribution after Sampling
0    9127071
1    9127071
Name: count, dtype: int64
Target class(test) distribution after Sampling
0    2281768
1    2281768
Name: count, dtype: int64
```



Modeling

Random Forest Classifier (RFC)

Ensemble learning for robust classification.

Captures complex relationships in data.

High performance and scalability.

Nearest Neighbors (KNN)

Instance-based learning for pattern recognition.

K-nearest neighbors influence classification.

Effective in high-dimensional spaces.

Support Vector Machine (SVM)

Maximize the margin between data points.

Effective for both linear and non-linear data.

Strong in handling high-dimensional data.

Ensemble Techniques

- Ensemble technique combining predictions of multiple models (classifiers).

RF + KNN = VC-1
- **Accuracy: 0.98**

KNN + SVM = VC-2
- **Accuracy: 0.82**

RF + SVM = VC-3
- **Accuracy: 1.00**

Voting Classifier
- Soft
  - majority of votes
- Hard
  - highest average probability

Model Deployment

[DDOS Prediction Application]

Front End	**Version Control System**	**IDE**	**Database/Storage**
Streamlit	GIT	Spyder	S3

Conclusion

1

ML models (RF, KNN, SVM, ensembles) enhance IoT security against DDoS attacks.

2

Behavior analysis provides insights for risk identification and mitigation.

3

A preventive approach strengthens IoT security against DDoS crimes.

Future Scope

Assess scalability on larger datasets to recognize IoT devices.

Explore more features and strategies for IoT network behavior analysis.

Evaluate robustness under varying networks and new IoT devices.

Build backup ML security solutions to deliver reliable, protected IoT services.


THANK YOU!
Q&A