Features:

Flow Duration
Flow Bytes/s
Flow Packets/s
Flow IAT Mean/Std/Max/Min
Subflow Fwd Packets/Bytes
Subflow Bwd Packets/Bytes
Active Mean/Min/Max/Std
Idle Mean/Min/Max/Std
Down/Up Ratio
Average Packet Size
Packet Length Min/Max/Mean/Std/Variance
Flag Count FIN/SYN/RST/PSH/ACK/URG/CWE/ECE
Fwd Packet Length Mean/Std/Max/Min
Fwd IAT Total/Mean/Std/Max/Min
Fwd Header Length
Fwd Packets/s
Fwd PSH/URG Flags
Avg Fwd Segment Size
Fwd Header Length.1
Fwd Avg Bytes/Bulk - Packets/Bulk - Bulk Rate
Bwd Packet Length Mean/Std/Max/Min
Bwd IAT Total/Mean/Std/Max/Min
Bwd Header Length
Avg Bwd Segment Size
Bwd Packets/s
Bwd PSH/URG Flags
Bwd Avg Bytes/Bulk - Packets/Bulk - Bulk Rate

Total Fwd/Backward Packets
Total Length of Fwd/Backward Packets

Init_Win_bytes_forward/backward
act_data_pkt_fwd
min_seg_size_forward

Labels:
'BENIGN', 'Bot', 'DDoS', 'DoS GoldenEye', 'DoS Hulk',
'DoS Slowhttptest', 'DoS slowloris', 'FTP-Patator', 'Heartbleed',
'Infiltration', 'PortScan', 'SSH-Patator',
'Web Attack - Brute Force', 'Web Attack - Sql Injection',
'Web Attack - XSS'

Level-1 Filtering

condition	Feature	Label (possible)
Destination Port =[80, 443]	Destination Port	Web Attack (all) 'Web Attack - Brute Force', 'Web Attack - Sql Injection', 'Web Attack - XSS'
Destination Port == 22	Destination Port	SSH-Patator
Destination Port == 21	Destination Port	FTP-Patator
Destination Port == anything other than the above four values (80,443,22,21)	Destination Port	User Data traffic

Level-2 Filtering

BENIGN: Normal traffic

```
if ['Destination Port'] in [80, 443] and ['Flow Duration'] < threshold:
    return 'BENIGN'

if ['Fwd Packet Length Max'] > threshold and ['Flow Packets/s'] > threshold:
    return 'DoS Hulk'

if ['Flow Packets/s'] > threshold and ['Total Fwd Packets'] > threshold:
    return 'DDoS'
```

PortScan: Scanning multiple ports to find an open port.

```
if ['Destination Port'] > threshold and ['Fwd IAT Max'] < threshold:
    return 'PortScan'

if ['Fwd Packets/s'] > threshold and ['Bwd Packet Length Max'] < threshold:
    return 'DoS GoldenEye'

if ['Destination Port'] == 21 and ['Fwd Packet Length Mean'] > threshold:
    return 'FTP-Patator'

if ['Fwd IAT Mean'] > threshold and ['Fwd IAT Max'] > threshold:
    return 'DoS slowloris'
```

```
if ['Destination Port'] == 80 and ['Fwd IAT Mean'] > threshold:
    return 'DoS Slowhttptest'

if ['Destination Port'] == 22 and ['Fwd Packet Length Mean'] > threshold:
    return 'SSH-Patator'

if ['Destination Port'] in [80, 443] and ['Fwd Packet Length Max'] > threshold:
    return 'Web Attack – XSS'

if ['Destination Port'] in [80, 443] and ['Fwd Packet Length Mean'] > threshold:
    return 'Web Attack - Brute Force'

if ['Destination Port'] in [80, 443] and ['Fwd Packet Length Std'] > threshold:
    return 'Web Attack – SQL Injection'

if ['Flow IAT Mean'] < threshold and ['Fwd Packets/s'] > threshold:
    return 'Bot'

if ['Total Length of Fwd Packets'] > threshold and ['Total Length of Bwd Packets'] > threshold:
    return 'Infiltration'

if ['Destination Port'] == 443 and ['Fwd Packet Length Max'] > threshold:
    return 'Heartbleed'
```

Flags

Flag Count FIN/SYN/RST/PSH/ACK/URG/CWE/ECE

SYN (Synchronize) Flag:

ACK (Acknowledgment) Flag:

- Normal/ BENIGN for balanced data traffic.
- A large number is DDoS

FIN (Finish) Flag:

RST (Reset) Flag:

PSH (Push) Flag:
URG (Urgent) Flag:
- Bot Traffic
-

CWE (Congestion Window Reduced) Flag:
ECE (ECN-Echo) Flag:

Counters;

IAT (Inter-Arrival Time)
- the time between the two flows
-

Sample Thresholds:
These thresholds are hypothetical and need to be validated and adjusted based on the specific dataset and the nature of the traffic being analyzed.

BENIGN:
threshold = 10000 (e.g., Flow Duration)

DoS Hulk:
threshold = 500 (e.g., Fwd Packet Length Max)

DDoS:
threshold = 1000 (e.g., Flow Packets/s)

PortScan:
threshold = 1024 (e.g., Destination Port)

DoS GoldenEye:
threshold = 200 (e.g., Fwd Packets/s)

FTP-Patator:
threshold = 150 (e.g., Fwd Packet Length Mean)

DoS slowloris:
threshold = 10000 (e.g., Fwd IAT Mean)

DoS Slowhttptest:
threshold = 5000 (e.g., Fwd IAT Mean)

SSH-Patator:
threshold = 100 (e.g., Fwd Packet Length Mean)

Web Attack – XSS:
threshold = 300 (e.g., Fwd Packet Length Max)

Web Attack - Brute Force:
threshold = 200 (e.g., Fwd Packet Length Mean)

Web Attack – SQL Injection:
threshold = 150 (e.g., Fwd Packet Length Std)

Bot:
threshold = 50 (e.g., Flow IAT Mean)

Infiltration:
threshold = 1000 (e.g., Total Length of Fwd Packets)

Heartbleed:
threshold = 200 (e.g., Fwd Packet Length Max)

,,,,,,,,,,,,,,,
Findings

Dataset: Training ULAK-Data-Set/Train_ULAK.csv'

Metric	Baseline Model	Model Customization (ML model with less complexity)	Accuracy >90%	Recall >90%	Precision >90%	False Positive value <10%
BENIGN	Random Forest					
DoS Hulk	Random Forest					
DDoS	Random Forest					
DoS GoldenEye	Random Forest					
DoS slowloris	Random Forest					
DoS Slowhttptest	Random Forest					
FTP-Patator	Random Forest					
SSH-Patator	Random Forest					
PortScan	Random Forest					
Bot	Random Forest					
Infiltration	Random Forest					
Heartbleed	Random Forest					
Web Attack – XSS	Random Forest					

Web Attack - Brute Force	Random Forest					
Web Attack – Sql Injection	Random Forest					

Dataset: Test ULAK-Data-Set/Test_ULAK.csv'

Metric	Baseline Model	Model Customization (ML model with less complexity)	Accuracy >90%	Recall >90%	Precision >90%	False Positive value <10%
BENIGN						
DoS Hulk						
DDoS						
DoS GoldenEye						
DoS slowloris						
DoS Slowhttptest						
FTP-Patator						
SSH-Patator						
PortScan						
Bot						
Infiltration						
Heartbleed						
Web Attack – XSS						
Web Attack - Brute Force						

Web Attack – Sql Injection						