Features set of each dataset.

CIC-IDS-2017 dataset

|  |  |  |
| --- | --- | --- |
| Flow ID | Bwd IAT Total | Fwd Header Length.1 |
| Source IP | Bwd IAT Mean | Fwd Avg Bytes/Bulk |
| Source Port | Bwd IAT Std | Fwd Avg Packets/Bulk |
| Destination IP | Bwd IAT Max | Fwd Avg Bulk Rate |
| Destination Port | Bwd IAT Min | Bwd Avg Bytes/Bulk |
| Protocol | Fwd PSH Flags | Bwd Avg Packets/Bulk |
| Timestamp | Bwd PSH Flags | Bwd Avg Bulk Rate |
| Flow Duration | Fwd URG Flags | Subflow Fwd Packets |
| Total Fwd Packets | Bwd URG Flags | Subflow Fwd Bytes |
| Total Backward Packets | Fwd Header Length | Subflow Bwd Packets |
| Total Length of Fwd Packets | Bwd Header Length | Subflow Bwd Bytes |
| Total Length of Bwd Packets | Fwd Packets/s | Init\_Win\_bytes\_forward |
| Fwd Packet Length Max | Bwd Packets/s | Init\_Win\_bytes\_backward |
| Fwd Packet Length Min | Min Packet Length | act\_data\_pkt\_fwd |
| Fwd Packet Length Mean | Max Packet Length | min\_seg\_size\_forward |
| Fwd Packet Length Std | Packet Length Mean | Active Mean |
| Bwd Packet Length Max | Packet Length Std | Active Std |
| Bwd Packet Length Min | Packet Length Variance | Active Max |
| Bwd Packet Length Mean | FIN Flag Count | Active Min |
| Bwd Packet Length Std | SYN Flag Count | Idle Mean |
| Flow Bytes/s | RST Flag Count | Idle Std |
| Flow Packets/s | PSH Flag Count | Idle Max |
| Flow IAT Mean | ACK Flag Count | Idle Min |
| Flow IAT Std | URG Flag Count | Label |
| Flow IAT Max | CWE Flag Count |  |
| Flow IAT Min | ECE Flag Count |  |
| Fwd IAT Total | Down/Up Ratio |  |
| Fwd IAT Mean | Average Packet Size |  |
| Fwd IAT Std | Avg Fwd Segment Size |  |
| Fwd IAT Max | Avg Bwd Segment Size |  |
| Fwd IAT Min |  |  |

Fwd Header Length.1 is a duplicate feature of Fwd Header Length.

|  |  |
| --- | --- |
| BENIGN | 440031 |
| DoS Hulk | 231073 |
| DoS GoldenEye | 10293 |
| DoS slowloris | 5796 |
| DoS Slowhttptest | 5499 |
| Heartbleed | 11 |

Missing data 1008 / 692703

Ton\_Iot\_Network Dataset

|  |  |  |
| --- | --- | --- |
| ts | dst\_ip\_bytes | http\_trans\_depth |
| src\_ip | dns\_query | http\_method |
| src\_port | dns\_qclass | http\_uri |
| dst\_ip | dns\_qtype | http\_version |
| dst\_port | dns\_rcode | http\_request\_body\_len |
| proto | dns\_AA | http\_response\_body\_len |
| service | dns\_RD | http\_status\_code |
| duration | dns\_RA | http\_user\_agent |
| src\_bytes | dns\_rejected | http\_orig\_mime\_types |
| dst\_bytes | ssl\_version | http\_resp\_mime\_types |
| conn\_state | ssl\_cipher | weird\_name |
| missed\_bytes | ssl\_resumed | weird\_addl |
| src\_pkts | ssl\_established | weird\_notice |
| src\_ip\_bytes | ssl\_subject | label |
| dst\_pkts | ssl\_issuer | type |

|  |  |
| --- | --- |
| normal | 300000 |
| scanning | 20000 |
| dos | 20000 |
| injection | 20000 |
| ddos | 20000 |
| password | 20000 |
| xss | 20000 |
| ransomware | 20000 |
| backdoor | 20000 |
| mitm | 1043 |

Missing data: 0/461043

KDD99

|  |  |  |
| --- | --- | --- |
| duration | su\_attempted | same\_srv\_rate |
| protocol\_type | num\_root | diff\_srv\_rate |
| service | num\_file\_creations | srv\_diff\_host\_rate |
| flag | num\_shells | dst\_host\_count |
| src\_bytes | num\_access\_files | dst\_host\_srv\_count |
| dst\_bytes | num\_outbound\_cmds | dst\_host\_same\_srv\_rate |
| land | is\_host\_login | dst\_host\_diff\_srv\_rate |
| wrong\_fragment | is\_guest\_login | dst\_host\_same\_src\_port\_rate |
| urgent | count | dst\_host\_srv\_diff\_host\_rate |
| hot | srv\_count | dst\_host\_serror\_rate |
| num\_failed\_logins | serror\_rate | dst\_host\_srv\_serror\_rate |
| logged\_in | srv\_serror\_rate | dst\_host\_rerror\_rate |
| num\_compromised | rerror\_rate | dst\_host\_srv\_rerror\_rate |
| root\_shell | srv\_rerror\_rate | outcome |

|  |  |
| --- | --- |
| smurf | 280790 |
| neptune | 107201 |
| normal | 97278 |
| back | 2203 |
| satan | 1589 |
| ipsweep | 1247 |
| portsweep | 1040 |
| warezclient | 1020 |
| teardrop | 979 |
| pod | 264 |
| nmap | 231 |
| guess\_passwd | 53 |
| buffer\_overflow | 30 |
| land | 21 |
| warezmaster | 20 |
| imap | 12 |
| rootkit | 10 |
| loadmodule | 9 |
| ftp\_write | 8 |
| multihop | 7 |
| phf | 4 |
| perl | 3 |
| spy | 2 |

Missing data: 0/494021