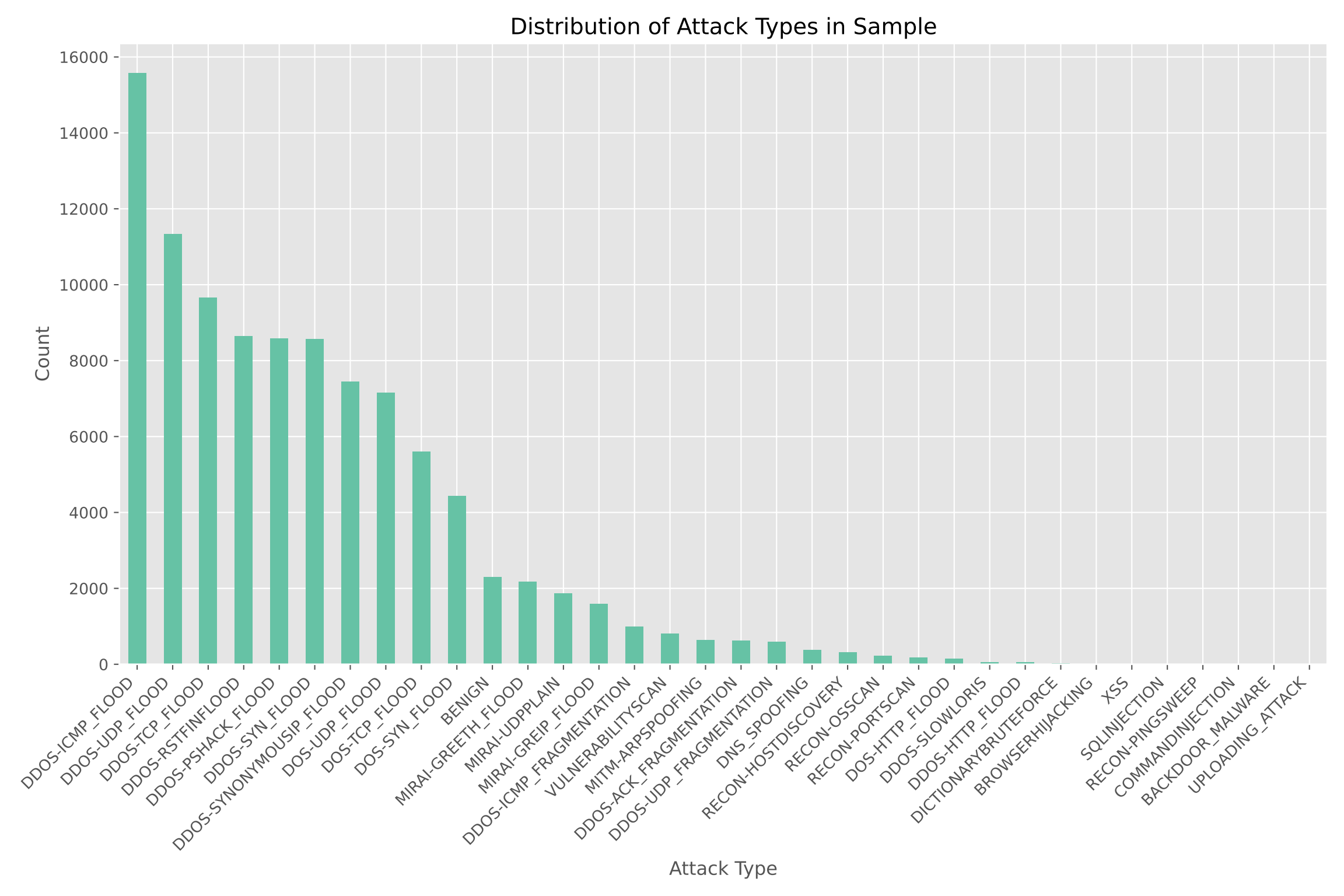
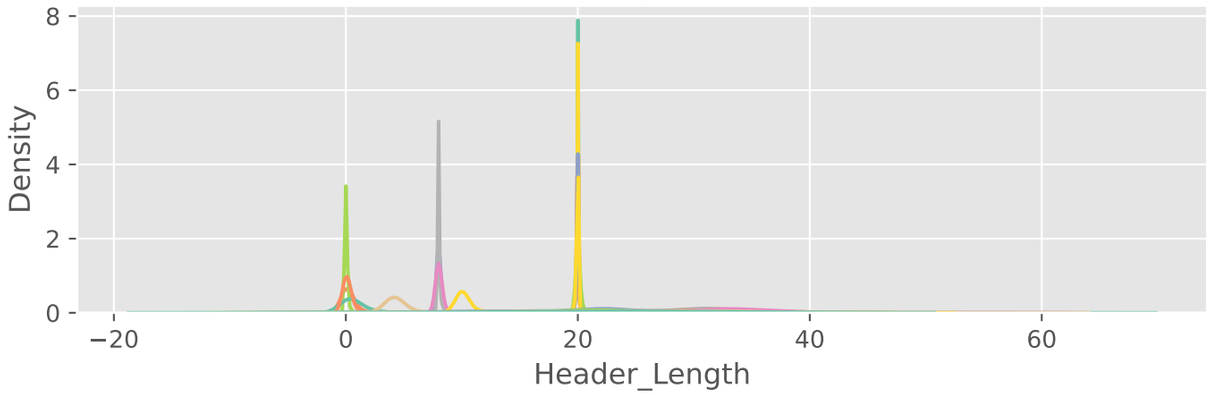
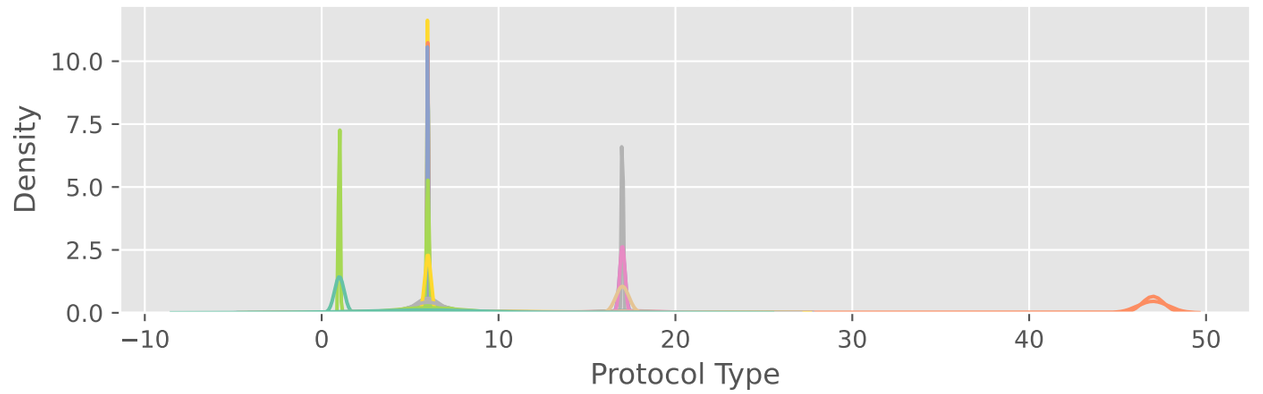
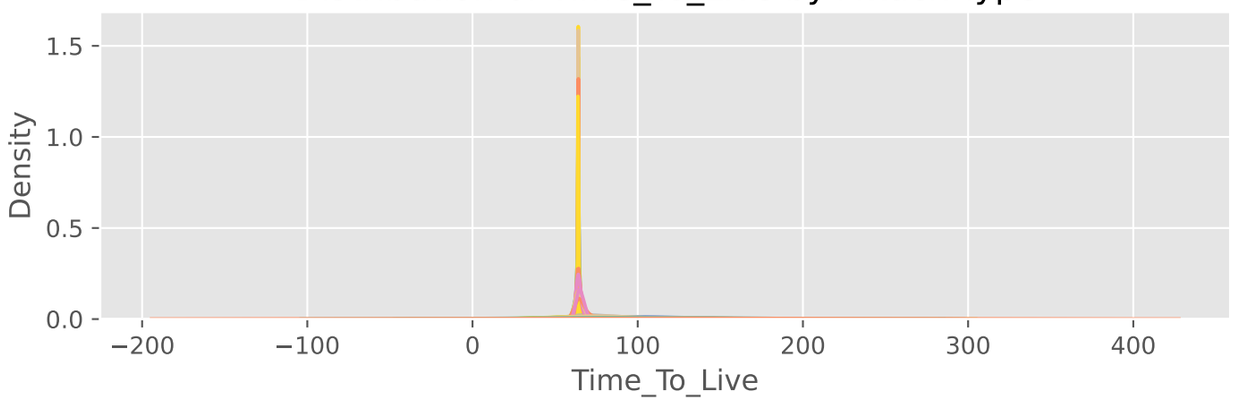
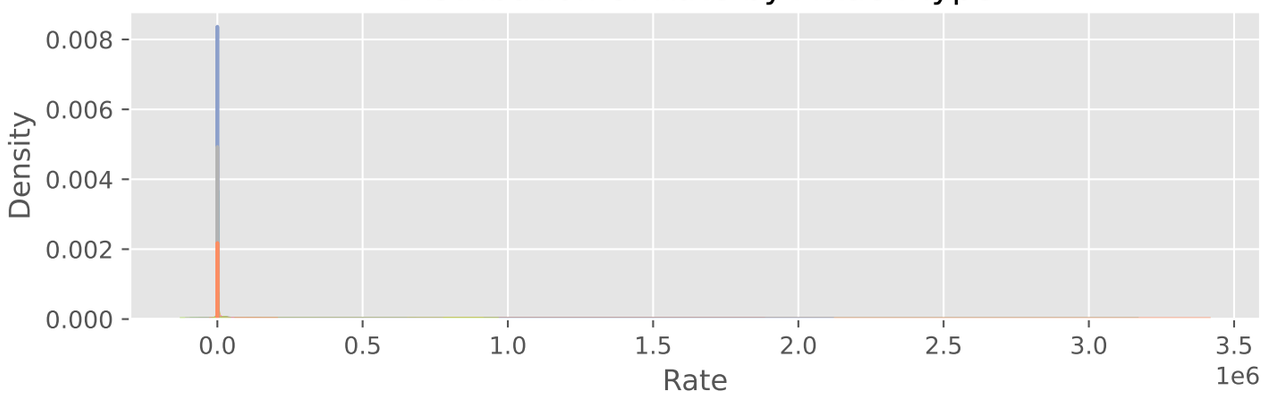

Distribution of Attack Types in Sample
Count
Attack Type
0
2000
4000
6000
8000
10000
12000
14000
16000
DDOS-ICMP_FLOOD
DDOS-UDP_FLOOD
DDOS-TCP_FLOOD
DDOS-RSTFINFLOOD
DDOS-PSHACK_FLOOD
DDOS-SYN_FLOOD
DDOS-SYNONYMOUSIP_FLOOD
DOS-UDP_FLOOD
DOS-TCP_FLOOD
DOS-SYN_FLOOD
BENIGN
MIRAI-GREETH_FLOOD
MIRAI-UDPPLAIN
MIRAI-GREIP_FLOOD
DDOS-ICMP_FRAGMENTATION
VULNERABILITYSCAN
MITM-ARPSPOOFING
DDOS-ACK_FRAGMENTATION
DDOS-UDP_FRAGMENTATION
DNS_SPOOFING
RECON-HOSTDISCOVERY
RECON-OSSCAN
RECON-PORTSCAN
DOS-HTTP_FLOOD
DDOS-SLOWLORIS
DDOS-HTTP_FLOOD
DICTIONARYBRUTEFORCE
BROWSERHIJACKING
XSS
SQLINJECTION
RECON-PINGSWEEP
COMMANDINJECTION
BACKDOOR_MALWARE
UPLOADING_ATTACK

The bar chart shows the distribution of different attack types in the CIC-IoT dataset sample.
This visualization helps us understand the class balance in the dataset, which is crucial for training effective machine learning models. Imbalanced classes might require special handling
like stratified sampling, class weighting, or oversampling techniques. The chart identifies the most common attack types in the dataset, providing insights into the threat landscape faced by SMEs deploying IoT devices.


Distribution of Header_Length by Attack Type
Density
Header_Length


Distribution of Protocol Type by Attack Type
Density
Protocol Type


Distribution of Time_To_Live by Attack Type
Density
Time_To_Live

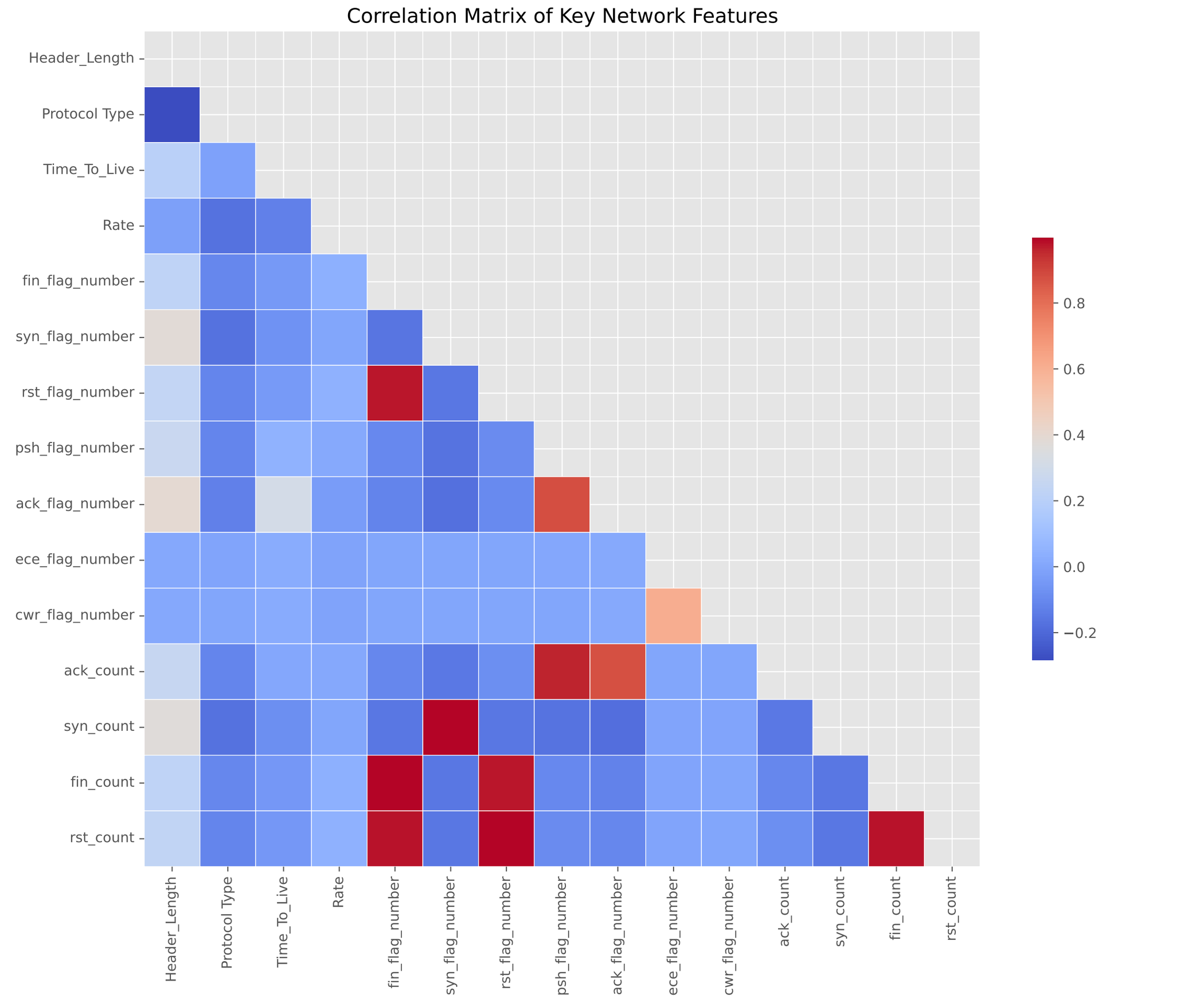

Distribution of Rate by Attack Type
Density
Rate
1e6

Distribution of fin_flag_number by Attack Type
Density
fin_flag_number

Distribution of syn_flag_number by Attack Type
Density
syn_flag_number

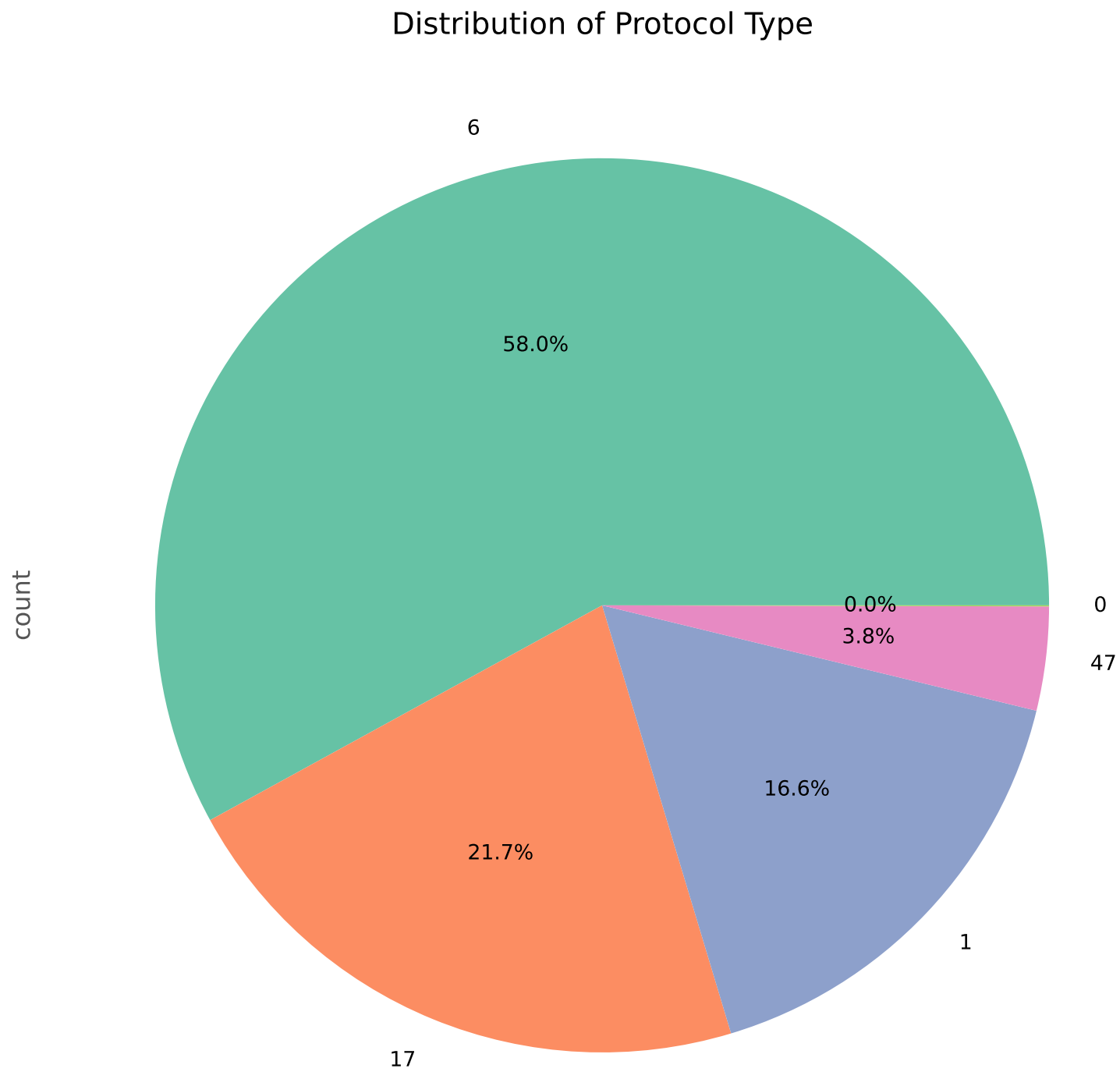
DDOS-PSHACK_FLOOD
MIRAI-GREIP_FLOOD
DOS-UDP_FLOOD
DNS_SPOOFING
DDOS-ICMP_FLOOD
DDOS-TCP_FLOOD
DDOS-SYN_FLOOD
DDOS-UDP_FLOOD
MITM-ARPSPOOFING
DDOS-SYNONYMOUSIP_FLOOD
DOS-TCP_FLOOD
VULNERABILITYSCAN
DOS-SYN_FLOOD
DDOS-RSTFINFLOOD
BENIGN
DDOS-SLOWLORIS
DDOS-ICMP_FRAGMENTATION
MIRAI-GREETH_FLOOD
RECON-HOSTDISCOVERY
MIRAI-UDPPLAIN
RECON-PORTSCAN
DDOS-ACK_FRAGMENTATION
DDOS-UDP_FRAGMENTATION
RECON-OSSCAN
BACKDOOR_MALWARE
DOS-HTTP_FLOOD
XSS
DDOS-HTTP_FLOOD
BROWSERHIJACKING
SQLINJECTION

This multi-panel visualization shows the distribution of six key network features across different attack types. The density plots reveal how feature distributions vary between benign traffic and different attack categories. Distinct patterns in these distributions can serve as important indicators for attack detection. Features with minimal overlap between attack and benign traffic are likely to be more valuable for classification tasks. These visualizations help in identifying the network characteristics that are most affected by different types of IoT attacks.


Correlation Matrix of Key Network Features
Header_Length
Protocol Type
Time_To_Live
Rate
fin_flag_number
syn_flag_number
rst_flag_number
psh_flag_number
ack_flag_number
ece_flag_number
cwr_flag_number
ack_count
syn_count
fin_count
rst_count
0.8
0.6
0.4
0.2
0.0
−0.2

The correlation heatmap displays the relationships between key network features in the CIC-IoT
dataset. Strongly correlated features appear in darker colors, with positive correlations in red

and negative correlations in blue. This visualization helps identify redundant features that might
be providing similar information, which is valuable for feature selection in machine learning model development. Strong correlations between features and specific attack types can also provide
insights into the network behaviors that characterize different IoT security threats, aiding in the development of effective detection mechanisms.


Distribution of Protocol Type
6
58.0%
0
0.0%
3.8%
47
16.6%
1
21.7%
17
count

This pie chart illustrates the distribution of network protocols in the CIC-IoT dataset as represented by the Protocol Type feature. Understanding protocol usage is crucial for IoT security
analysis as different protocols have varying security implications and vulnerabilities. Attackers often target specific protocols, and unusual protocol distributions can indicate potential security threats. For SMEs deploying IoT devices, this visualization highlights which protocols are most commonly used in their environments and consequently which might
require additional security controls or monitoring.