# IoT Network Intrusion Detection Analysis

**INFO 526 - Fall 2024 - Project 01**
**Team: ViZZards**


Members:

Vik Ruhil,

Raghav Upadhyay,

Chaitanya Suralkar,

Tushar Shrivastava

Yash Sharma,

Partha Vemuri,

Smit Shah


# Topic and Motivation

- **Motivation**: The growing adoption of IoT devices has revolutionized industries but also exposed networks to increased cybersecurity threats.
- **Problem**: Limited security features in IoT devices make them vulnerable to sophisticated cyberattacks such as DDoS, Brute-Force, and ARP Poisoning.
- **Objective**: To identify patterns and anomalies in IoT network behaviors during attacks, contributing to the development of robust intrusion detection systems (IDS).

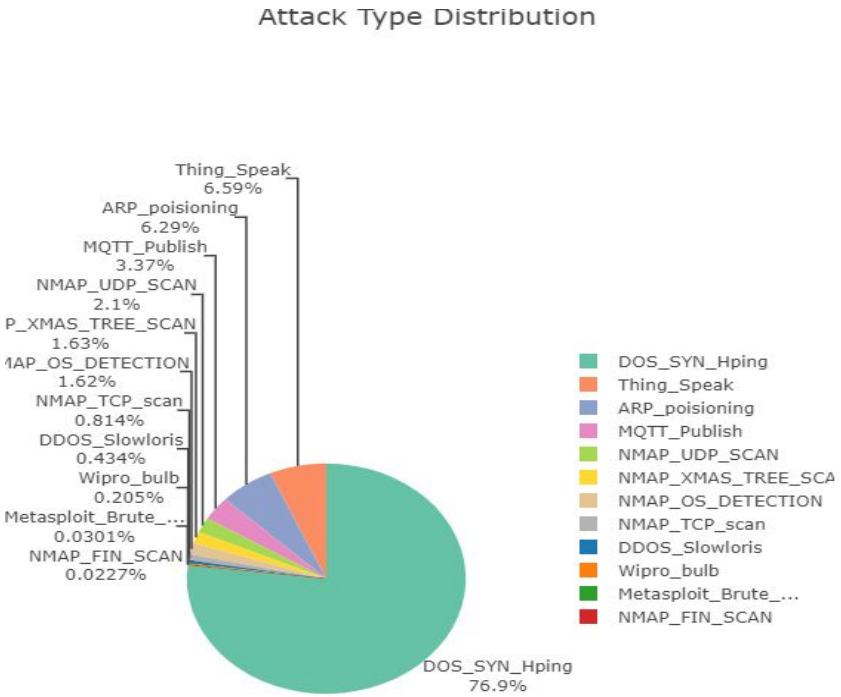
# Data

**Dataset**: RT-IoT 2022 (UCI Machine Learning Repository)

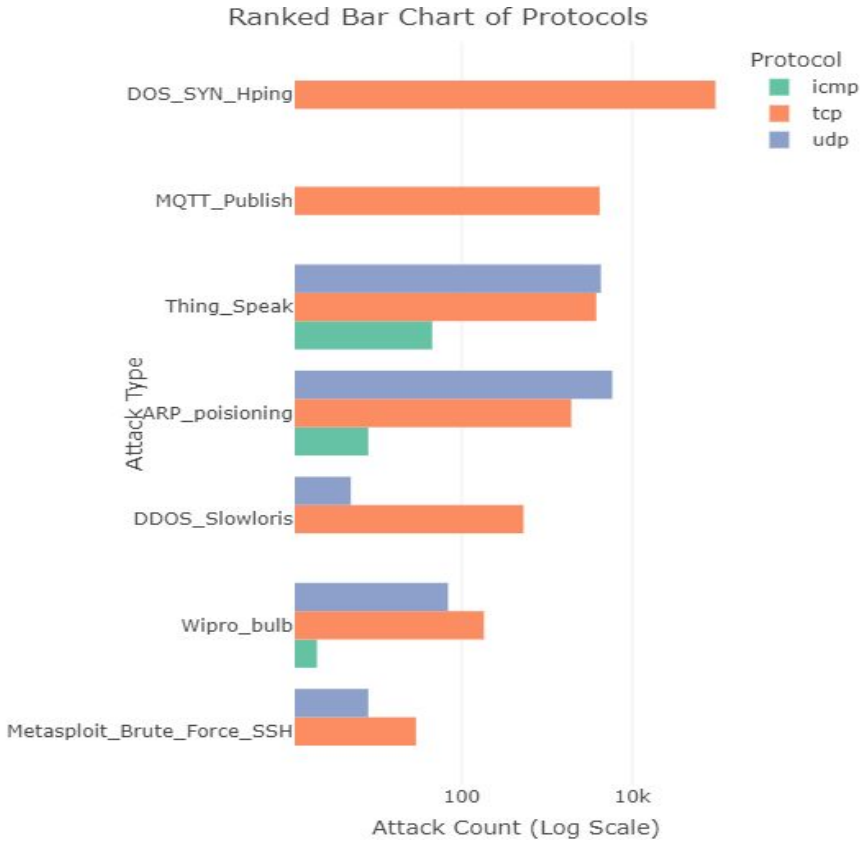
- **Size**: 123,117 rows, 77 columns
- **Features**: Captures both normal and malicious IoT network traffic.
  - **Devices**: ThingSpeak-LED, Wipro Bulb, MQTT-Temp, Amazon Alexa.
  - **Attack Scenarios**: Brute-Force SSH, DDoS (Hping, Slowloris), Nmap scans.
  - **Metrics**: Protocol usage, bandwidth, payload size, inter-arrival times, flow characteristics.
- **Preprocessing**: Fully cleaned, structured, and ready for analysis.

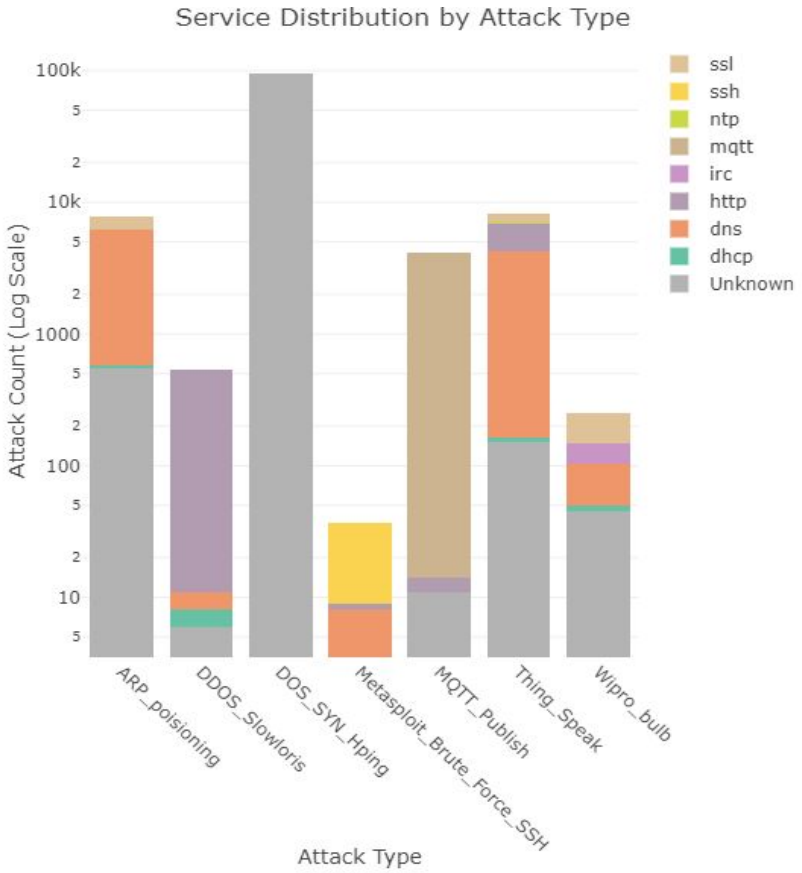
# Highlights from EDA

- **Protocol Usage**:
  - DDoS attacks heavily utilize TCP and UDP protocols.
- **Bandwidth Anomalies**:
  - Significant spikes in metrics like `fwd_pkts_tot` and `bwd_pkts_per_sec` during attacks.
- **Payload Characteristics**:
  - Extreme payload sizes observed during malicious activity.
- **Inter-arrival Times**:
  - Irregular timing patterns in metrics like `fwd_iat.min`.
- **Flow Flags**:
  - Repeated TCP SYN messages (e.g., Slowloris attacks).

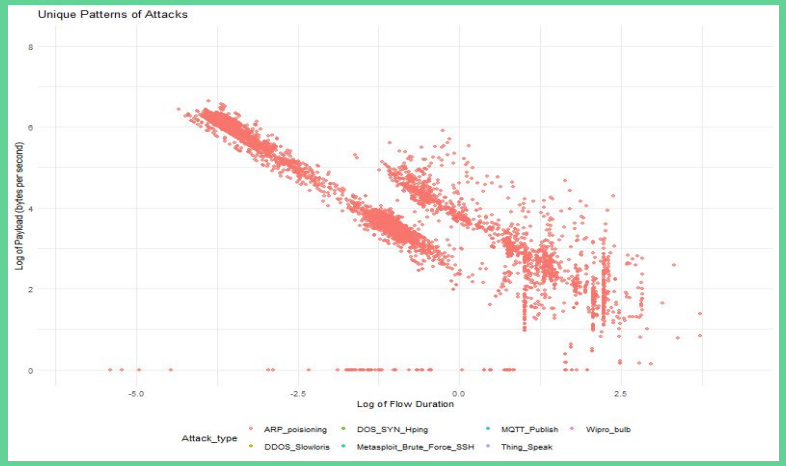


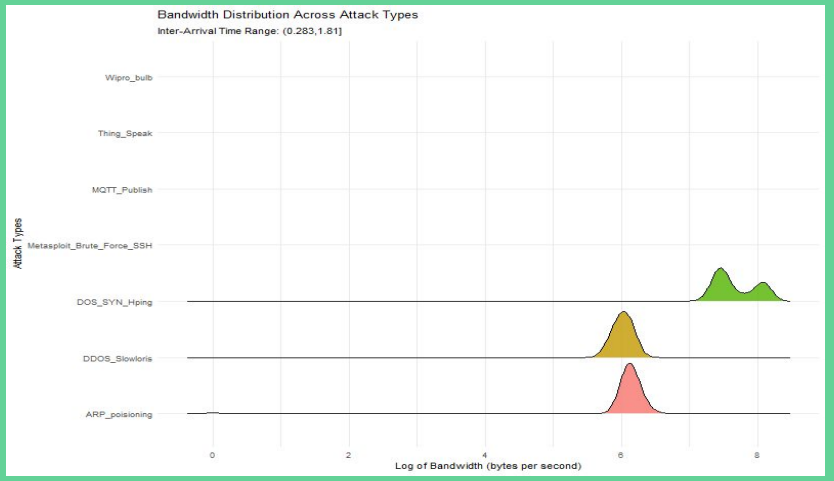
# Visualizations Q1

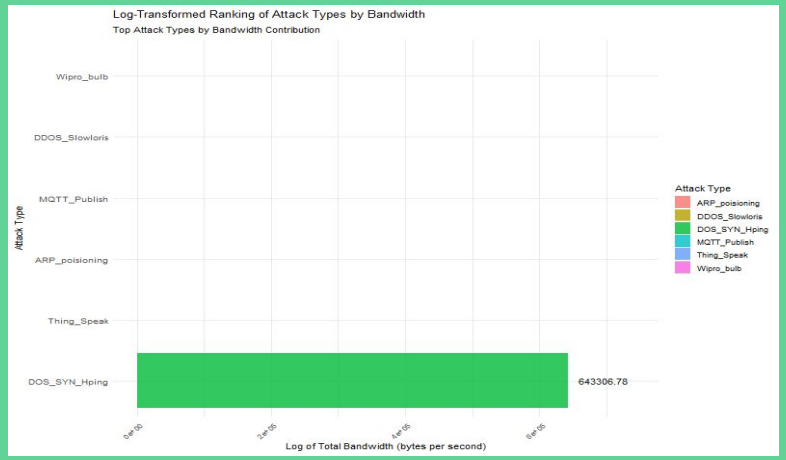


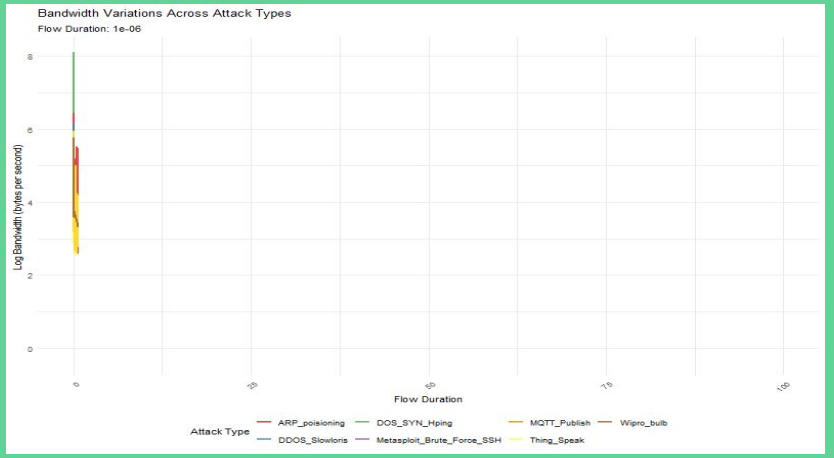



# Visualizations For Q2

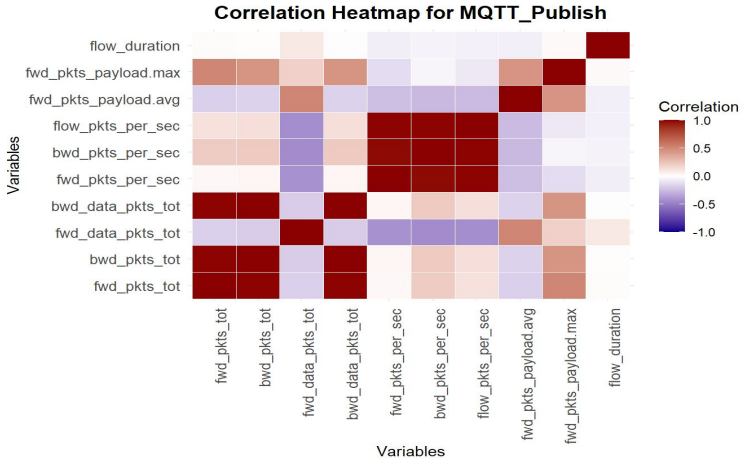


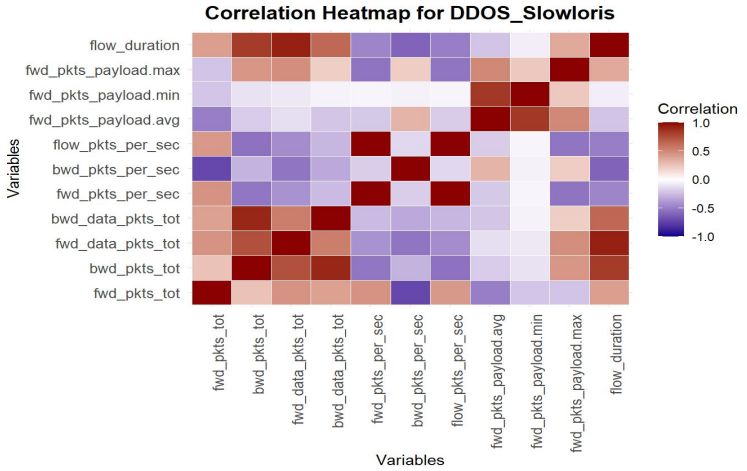



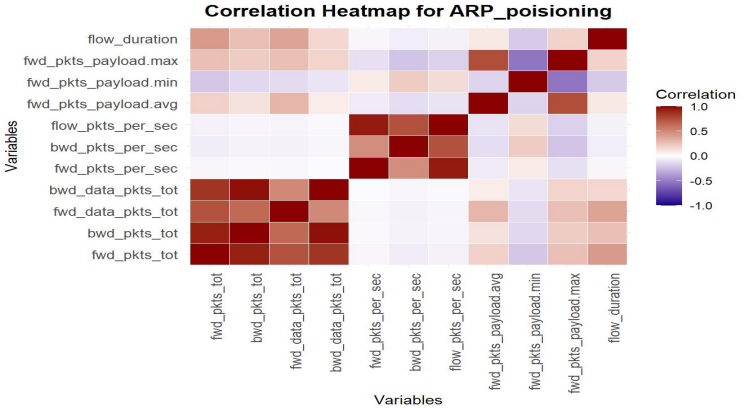



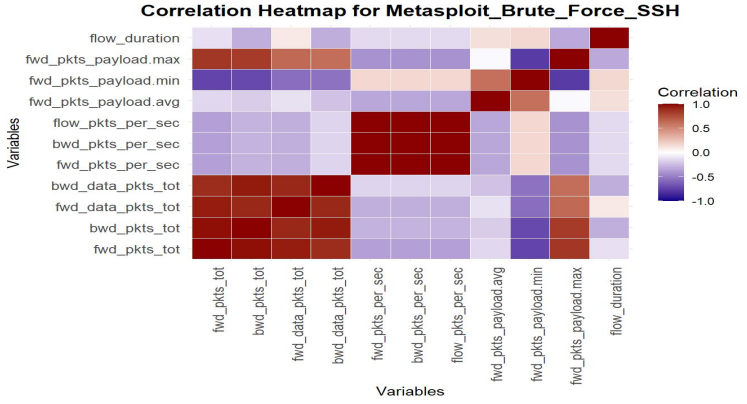



# Visualizations Q3



# Conclusions and Future Work

In conclusion, our analysis highlights critical insights into attack patterns and their implications for cybersecurity. High bandwidth and rapid flows are characteristic of volumetric attacks, while long inter-arrival times point to resource-exhaustion tactics. Additionally, correlations between payload and flow patterns reveal stealthy attack behaviors that are often missed by conventional methods. These findings emphasize the significance of developing robust solutions, including attack fingerprinting to identify unique signatures, advanced anomaly detection systems for early threat identification, and tailored IoT defenses to address the specific vulnerabilities of connected devices.

**Future Work**:

- Create machine learning models to classify and predict attack types.
- Investigate device-specific attack vulnerabilities.
- Develop real-time attack monitoring tools for IoT networks.

**Limitation:** Missing source/destination data limits identification.