1. Introduction

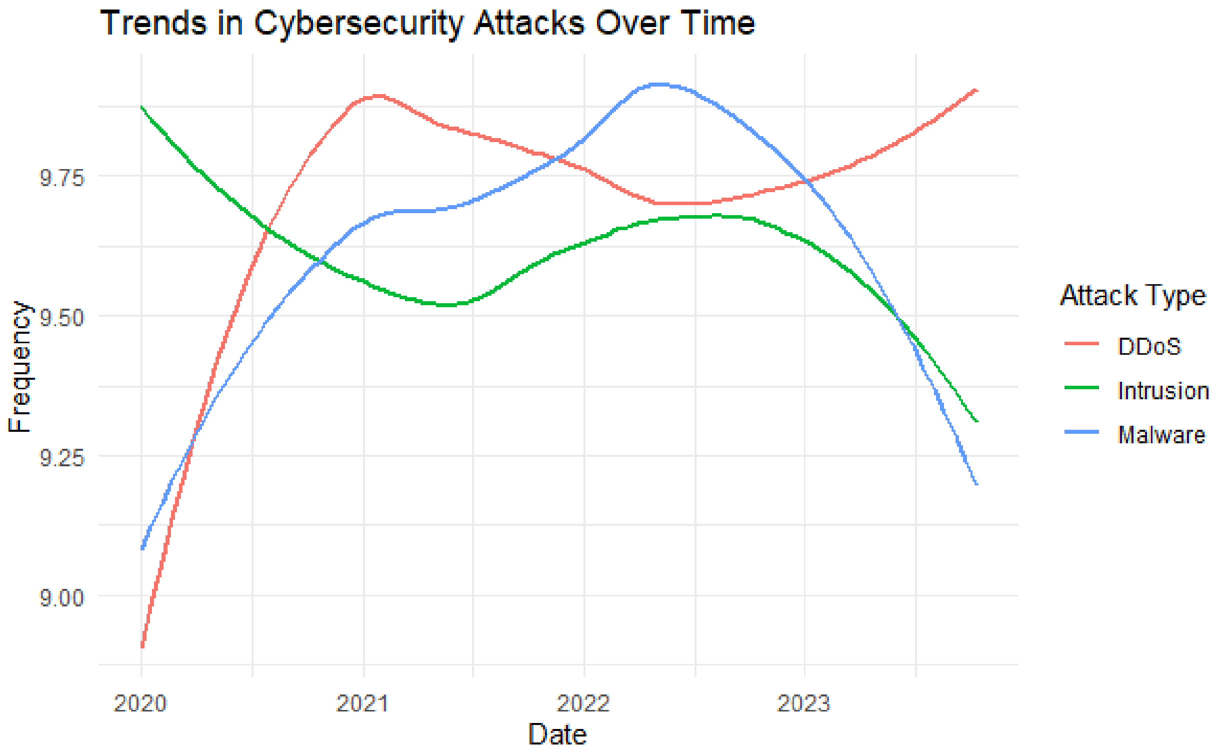
I am very interested in cyber security and because of that I decided that I wanted to dedicate this project to something related to cyber security. There is now a big emphasis on cyber security since we are all getting more and more into technology and companies are storing more and more data. In this project I examine a dataset of cyber attacks containing data on different attacks with a lot of information. I take a focus on Distributed Denial of Service attacks or DDoS attacks as during my research I found that they had a very high frequency of occurrence and usually have high severity. By analyzing trends, severity distributions, and packet characteristics, this report aims to provide insights into DDoS attacks.

2. Method

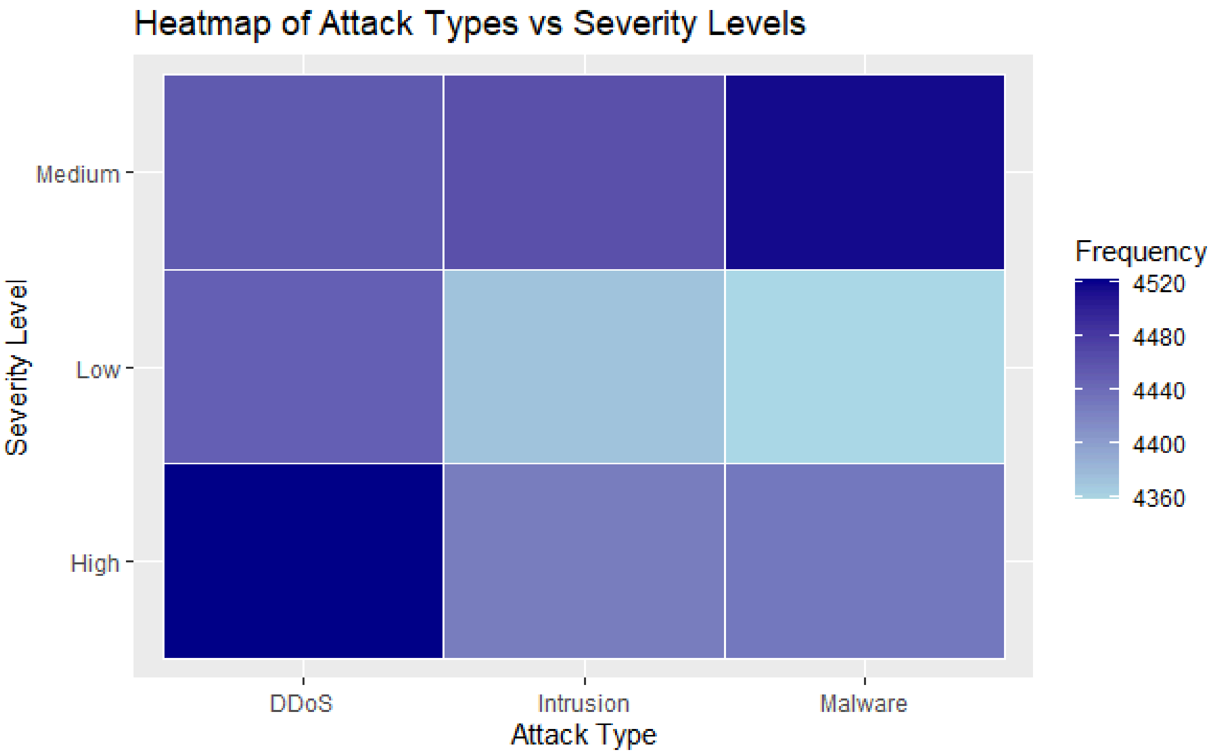
The dataset I chose to use for this project contained 40,000 cyber attacks as mentioned and they included many details that I used such as attack type, severity level, traffic type, and packet characteristics. I also had to do some data preprocessing which included, me having to parse the timestamp column into a date format to work with my trend lines, for visualization I had grouped data together by relevant attributes such as traffic type and severity level to be able to look at different patterns of attacks. The analysis I conducted was all using R and I included visualizations to explore trends, distributions, and geographic patterns specific graphs that I include are trends that analyze attacks over time, bar chart to identify top geolocations for DDoS attacks, as well as heat maps to examine different variables such as attack types and traffic types based on severity level.

3. Results and Discussion

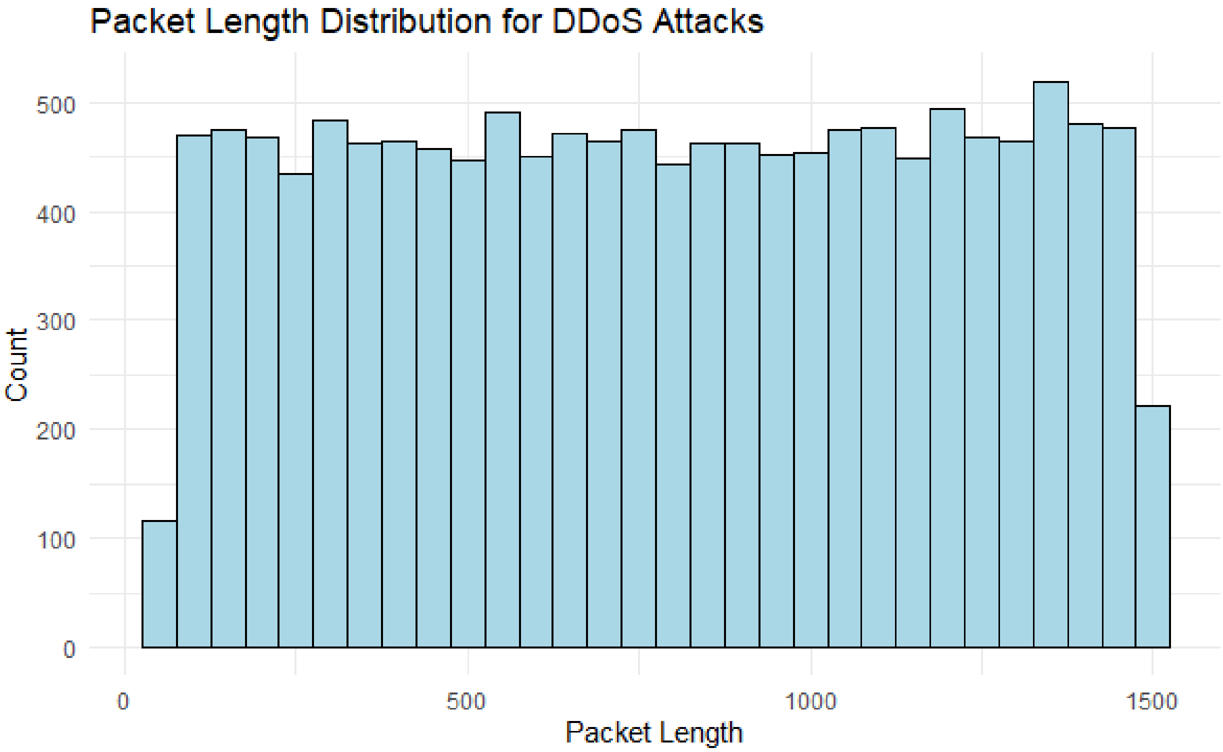
Trends in Cybersecurity Attacks Over Time



The trend analysis clearly shows that DDoS attacks have steadily increased over time, indicating a growing threat and on top of that you can see a very sharp decline of intrusion and malware attacks. DDoS attacks are consistently outpacing other attack types, showing the need for new scalable mitigation solutions.

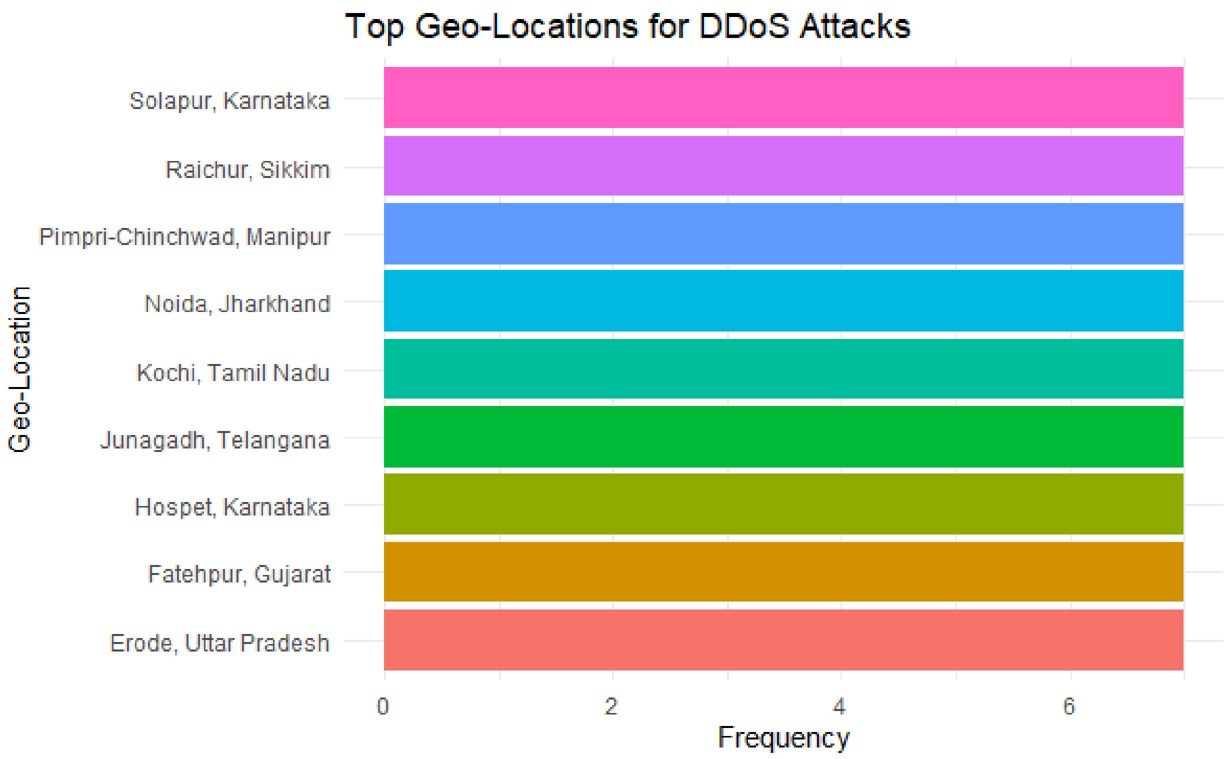

Heatmap of Attack Types vs Severity Levels
Severity Level
Medium
Low
High
DDoS
Intrusion
Malware
Attack Type
Frequency
4520
4480
4440
4400
4360

Packet Length Distribution



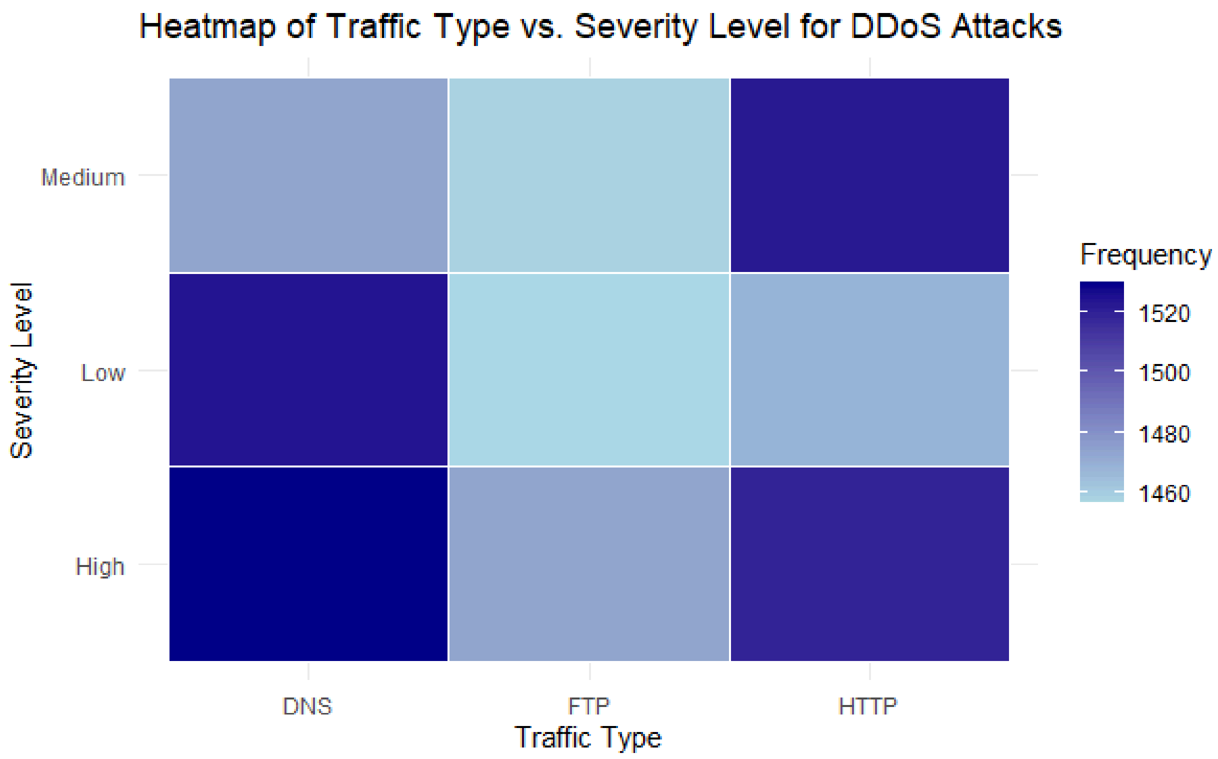
The distribution of packet lengths for DDoS attacks peaks around 500–1000 bytes, suggesting the use of specific tools or protocols. Understanding these patterns can aid in creating filters to block suspicious traffic during attacks.

Top Geo-Locations for DDoS Attacks



The geolocation analysis identified hotspots such as Erode (Uttar Pradesh) and Fatehpur (Gujarat). These regions may either serve as origins of attacks or targets. Collaborations with ISPs and regional authorities could help mitigate risks in these areas.

Traffic Type and Severity Levels



HTTP-based DDoS attacks were the most severe, likely due to their direct impact on web applications. DNS and FTP attacks also showed significant severity, though less frequent. This highlights the importance of deploying Web Application Firewalls (WAFs) and DNS security extensions to counter such threats.

4. Conclusion

This project highlights the importance of looking into data like this and also shows the increasing threat of DDoS attacks the plots I created show that these threat actors attack specific traffic patterns many attackers now are attacking the DNS traffic type which can mean many things but my guess is that attackers are trying to take down websites, email servers, and other critical services these attackers a lot of the time just want to cause economic impact. Another interesting fact that the data showed is that these attacks have a high geographic correlation with india and this does not mean that people from india are sending these attacks, this means that either systems in india are disproportionately targeted for DDoS attacks for certain reasons or it means that there are a ton of compromised devices or systems part of botnets that are located in India. Botnets are basically multiple compromised devices that these attackers use to send packets that disrupt network connections.