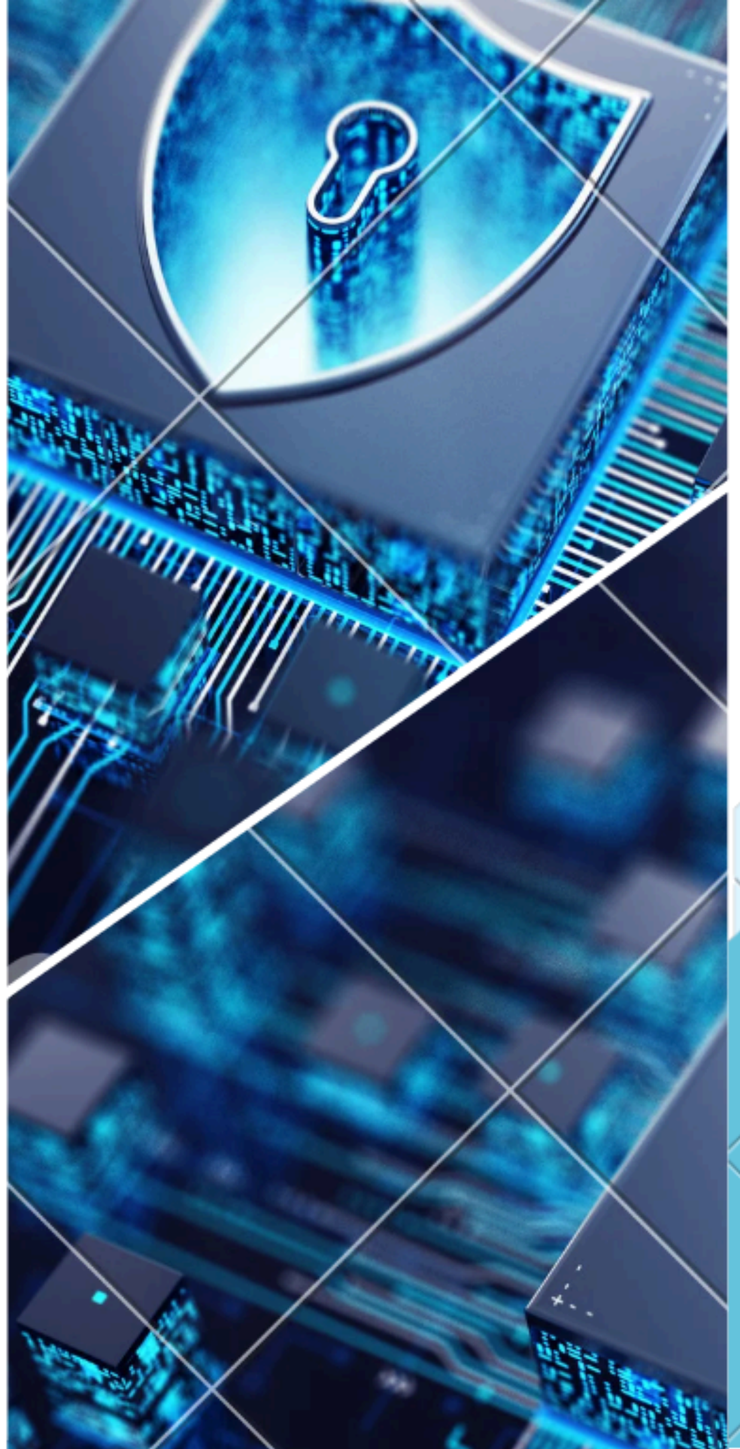
Cyber Sentinels

PROJECT NAME :

MOMMYNET

DDOS ATTACK PREVENTION TOOL

Presented By- **DEVASHISH | DINESH | SOURABH**



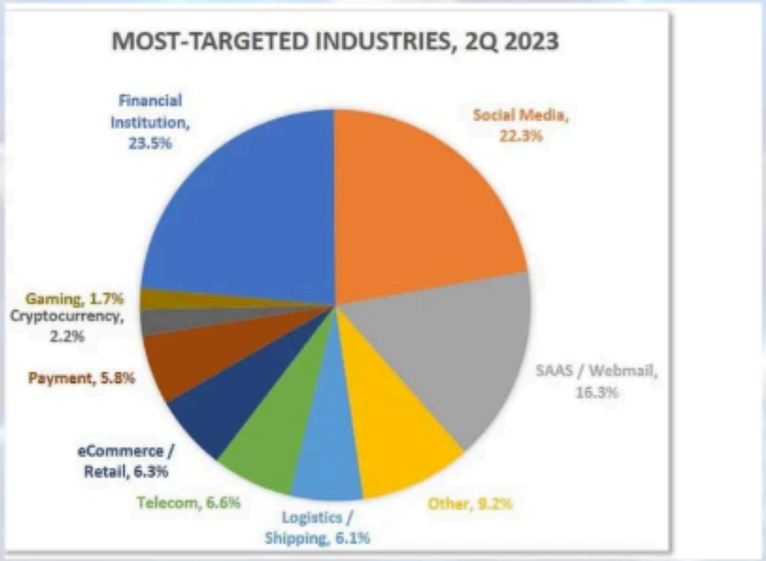
PROBLEM :

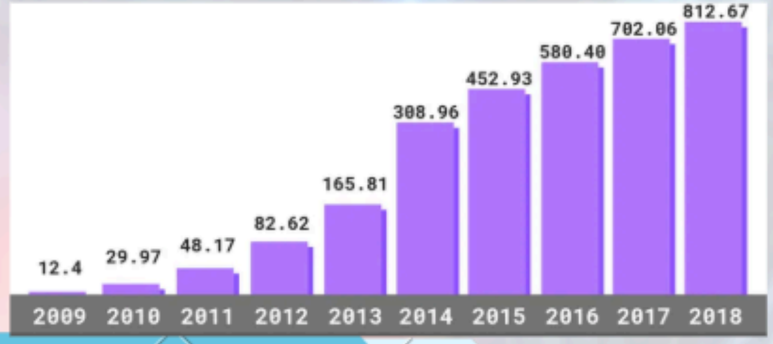
The problem in a DDoS attack is that it floods a target with overwhelming traffic, rendering it unavailable to legitimate users and disrupting services.

IDEA/SOLUTION :

- Proactively identifies DDoS attacks as they occur.
- Executes rapid & detailed analysis of traffic.
- Instantly protects critical infrastructure from attacks.
- Enhances security and ensures network reliability.
- Deploys targeted defenses with surgical precision.

Statistics :





PROCESS OF DOS ATTACK:

Socket Programming :

Used to Create Socket to connect attacker to server.

Tor Network/Cycle Identity :

It is integrated to hide the identity of the Attacker

Threading :

It is used to make excess load via sockets on the server.

DETECTION TECHNIQUES

ANOMALY DETECTION

Will detect all the anomalies happening on the server and network

BEHAVIOUR ANALYSIS

will analyse the behaviour of the request like it's speed and time

SIGNATURE-BASES DETECTION

Will match the signatures with the incoming requests like the packet size and count

LOG BASED ANALYSIS

WIll check all the server/website logs for the requested packets for advanced detection.

TRAFFIC ANALYSIS

It will analyze the whole traffic whether an attack or a legit request on the server so that attack can be prevented

MITIGATION TECHNIQUES :

Traffic Filtering

Filters True/Malicious Traffic.

SYN Flood Protection

Blocks SYN Flood Based Attacks.

Rate Limiting

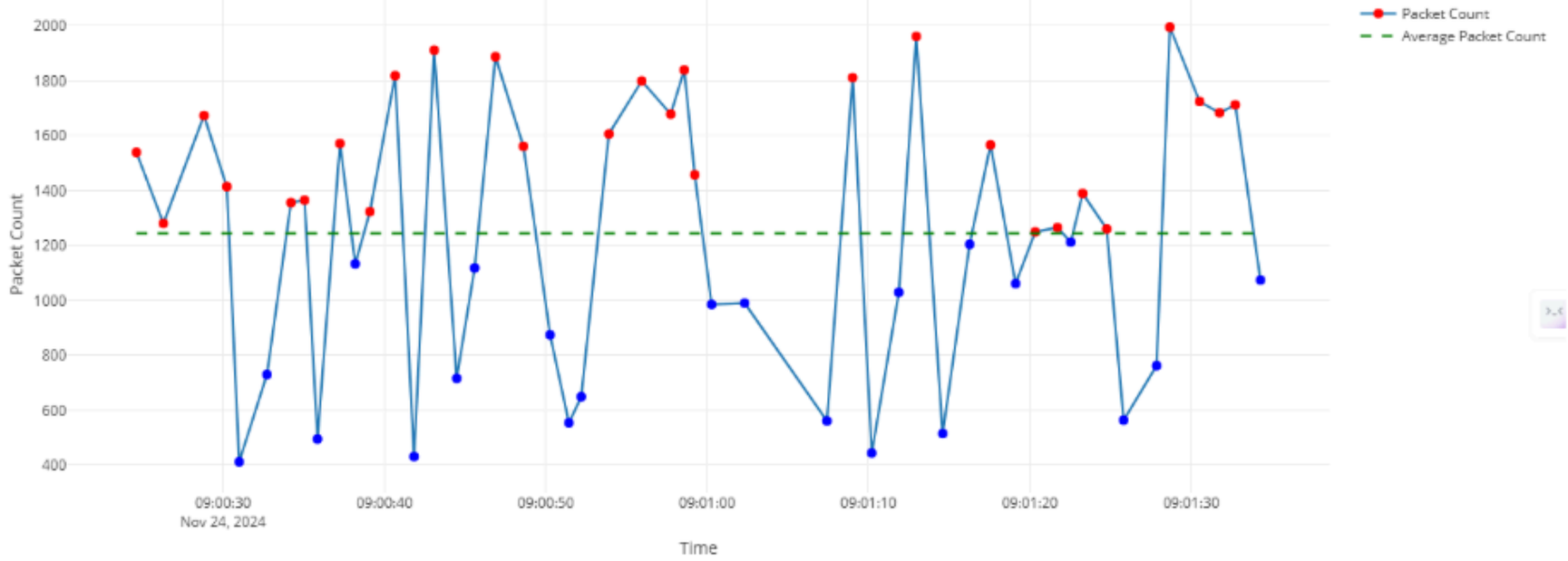
Slows Down the Network to reduce the request speed.

ICMP Rate Limiting

Internet Control Message protocol based Script Payload attacks.(Commonly known as slow attacks.)

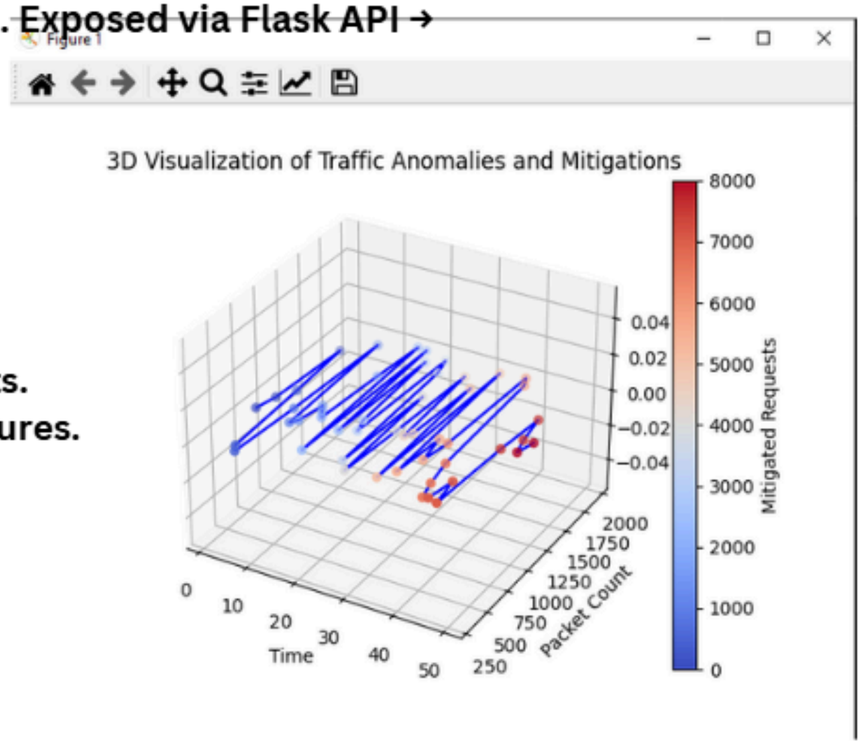
IP Blocking

Blocks the Sources from which the attacks are coming.



Graphical data of Anomalies detected on the server

Anomaly data collected → 2. Stored or processed with Pandas → 3. Exposed via Flask API →



Data Visualization

Chart Libraries:

Chart.js: Used for creating interactive bar, line, and pie charts.

Plotly.js: For advanced, dynamic charts with zoom and pan features.

TECHNOLOGY USED:

WORK FLOW OF THE MODEL:

POTENTIAL CHALLENGES AND RISKS :

- High-quality traffic data is essential for effective model training.
- The system may misclassify legitimate traffic or miss actual threats.
- Attackers may exploit vulnerabilities, reducing effectiveness against advanced threats.
- Adversarial Attacks.

FUTURE SCOPE :

- AI-driven threat detection enhancements
- Adaptive machine learning algorithms
- Proactive defense against new attacks
- Real-time predictive attack analysis
- Seamless integration with emerging technologies


THANK YOU
PRESENTED BY- CYBER SENTINELS
DEVASHISH | DINESH | SOURABH