THE DDOS DEFENDER

Due to the expansion of network infrastructure and the increasing dependency on online services have made networks susceptible to various cyber threats like distributed denial of service attacks commonly known as Ddos.

This type of attack disrupt the availability of services causing significant financial and reputational damage. I was really inspired to conceive a solution capable of surpassing the formidable challenge posed by the distributed denial of service attacks as a conventional rule based methodologies have grappled with their ineffectiveness in combating this pervasive threat.

The solution involved developing a model that is more adaptive and more intelligent than the convectional rule.

This project presents a comprehensive solution for DDos attack detection and mitigation utilizing machine learning techniques to identify anomalies behavior associated with DDos attack.

The Existing Gap In The field

Most routers and firewalls cannot perform the antispoofing and this makes them vulnerable .

finite capacity

When faced with an extremely large-scale attack, they may become overwhelmed, leading to service disruptions.

The system leverages features such as traffic volume, packet rates, and packet payload characteristics to create predictable model capable of distinguishing normal traffic from malicious traffic .

DATA COLLECTION

* Real-time network traffic data is collected from various sources, including network devices, servers and intrusion detection system.

THE ACTUAL SOLUTION

Feature Engineering   
The relevant features are extracted from the raw data, encompassing both statistical and deep packet inspection techniques to search for any anomalies.

Machine learning models

* Supervised models such as random forest and support vector machine are trained on labelled datasets to classify traffic as normal or malicious . Unsupervised models eg clustering algorithms are employed to detect anomalies pattern without labelled data.

Attack Mitigation

* Upon detection of a DDos attack, the system triggers appropriate mitigation strategies such as:

1. Traffic diversion
2. IP blocking
3. Rate limiting
4. Ri-routing traffic

Conclusion

In conclusion, this project represents a significant step forward in enhancing network security by harnessing the capabilities of machine learning to detect and mitigate DDos attacks, thereby ensuring an uninterrupted service availability in the face of evolving cyber threats.