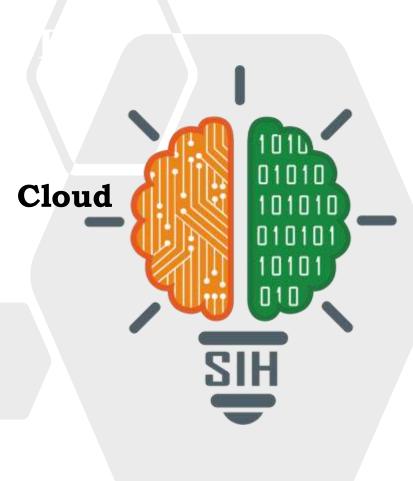# SMART INDIA HACKATHON 2024

- **Problem Statement ID – 1649**

- **DDOS Protection System for Cloud Architecture**

- **Blockchain and Cybersecurity**

- **Software**

- **Team ID-**

- **Creative Synergy**

DDOS Protection System for Cloud: Architecture and Tool

- DDoS Attack means "Distributed Denial-of-Service (DDoS) Attack" and it is a cybercrime
- DDoS attacks are on the rise, and even some of the largest global companies are not immune to being "DDoS'ed".
- A distributed denial of service (DDoS) attack is a brute-force attempt to slow down or completely crash a server.
- Although still a serious threat to businesses, increasing corporate awareness coupled with Internet security software enhancements has helped reduce the sheer number of attacks. Nonetheless, any denial of service represents a serious risk.

Types of DDOS attacks

TECHNICAL APPROACH

- Preventing DDoS attacks can be challenging, particularly during high-traffic periods or across a vast and distributed network architecture. A truly proactive DDoS threat defense hinges on several key factors: attack surface reduction, threat monitoring, and scalable DDoS mitigation tools.

- Before a cyberthreat is on your radar, you'll want to have a process for one in place. Preparedness is key to promptly detecting and remedying an attack.

Develop a denial-of-service defense strategy to help detect, prevent, and reduce DDoS attacks.

↓

Identify gaps in security and assess potential threats to your setup.

↓

Update any protection software or technology and ensure it's working correctly.

↓

Get your team on board and assign roles in the event of an attack.

The most obvious symptom of a DDoS attack is a site or service suddenly becoming slow or unavailable. But since a number of causes — such a legitimate spike in traffic — can create similar performance issues, further investigation is usually required.

Traffic analytics tools can help you spot some of these telltale signs of a DDoS attack:

- Suspicious amounts of traffic originating from a single IP address or IP range
- A flood of traffic from users who share a single behavioral profile, such as device type, geolocation, or web browser version etc

It's essential that you boost your efforts with products, processes, and services that help you secure your business. That way, once a threat is detected, your team is knowledgeable and empowered to act on it.

IMPACT AND BENEFITS

- Financial damage -
  The financial damage to businesses can be severe. A recent study by Kaspersky Lab revealed that a DDoS attack can cost a company over $1.6 million – a staggering sum for any company. A DDoS attack can almost be meant as a "smokescreen", diverting your staff's attention away while another attack, like data theft, is taking place.

Importance of DDos Protection-
This reinforces the importance of guarding against DDoS attacks at all costs and taking the necessary security procedures to avoid catastrophic financial losses.

- https://www.cloudflare.com/en-in/learning/ddos/what-is-a-ddos-attack/

- https://blackarch.org/dos.html

- https://github.com/Leeon123/golang-httpflood

- https://github.com/Aaron45421

- https://www.duckdns.org/why.jsp

- https://aaronofficial.gitbook.io/aaronofficial-docs/