SMART INDIA HACKATHON 2024

SMART INDIA HACKATHON 2024

DDoS Protection System for Cloud

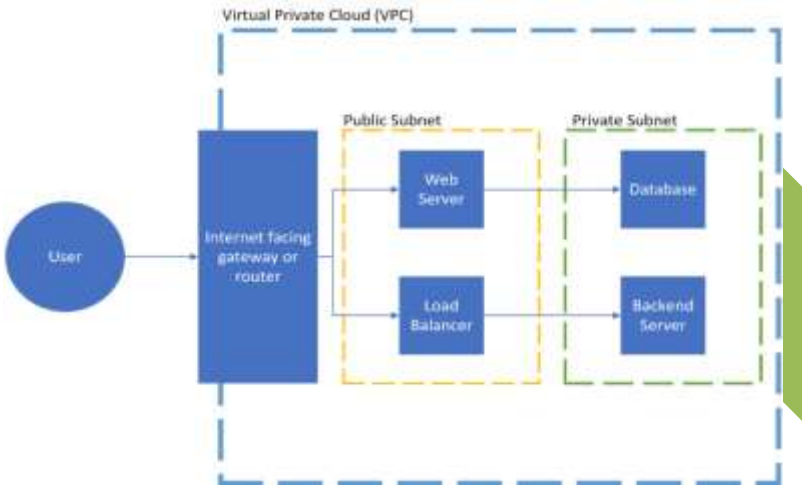
- **Problem Statement ID – 1649**
- **Problem Statement Title- DDoS Protection System for Cloud: Architecture and Tool**
- **Theme- Blockchain & Cybersecurity**
- **PS Category- Software**
- **Team ID-**
- **Team Name- Hexagon**

Hexagon

Problem Identification

SMART INDIA HACKATHON 2024

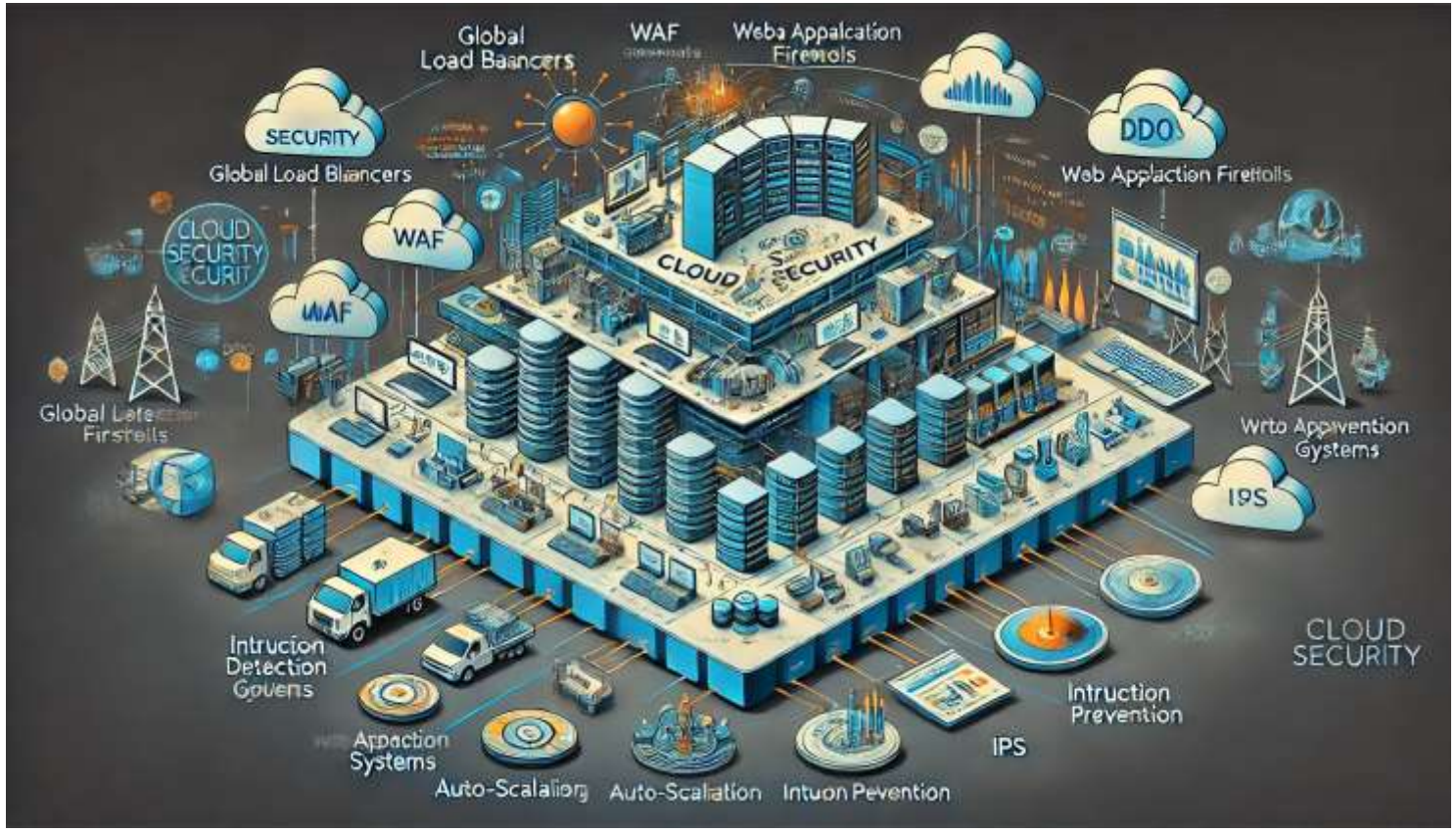
- Difficulty in distinguishing between legitimate traffic spikes and actual DDoS attacks.
- Detecting and identifying suspicious traffic originating from single IP addresses or specific IP ranges.
- Recognizing and analyzing abnormal traffic patterns and behaviors indicative of DDoS attacks.
- Protecting against diverse types of DDoS attacks originating both outside and within the cloud infrastructure.
- Preventing and mitigating attacks that target and disrupt the connection between clients and the webserver.
- Ensuring continuous high availability of services despite ongoing or attempted DDoS attacks.
- Developing automated tools capable of real-time detection, response, and recovery from DDoS attacks.
- Designing a resilient cloud architecture that can adapt to and withstand various and evolving DDoS attack strategies.



Hexagon

TECHNICAL APPROACH

SMART INDIA HACKATHON 2024



- Here is a visual representation of the technical approach, showcasing the multi-layered cloud security architecture designed to protect against DDoS attacks. This diagram highlights the various components and how they work together to ensure high availability and automated recovery during an attack.

Hexagon

FEASIBILITY AND VIABILITY

SMART INDIA HACKATHON 2024

- Technical Feasibility: Existing cloud tools like WAF and IDS make implementation technically viable.
- Economic Feasibility: Cost is justified by preventing significant losses from DDoS attacks.
- Operational Viability: Seamless integration with existing infrastructure ensures minimal disruption.
- Scalability: The architecture is designed to grow with the business, ensuring long-term viability.
- Implementation Complexity: Overcome by consulting cloud security experts.
- Evolving Threats: Mitigate through regular updates and continuous monitoring.

Hexagon

IMPACT AND BENEFITS

SMART INDIA HACKATHON 2024

- Enhanced security and trust from users due to robust DDoS protection.
- Business continuity with minimal downtime during attacks.
- Scalability to handle growing traffic without compromising security.
- Preservation of reputation by preventing service disruptions.
- Increased user confidence in interacting with online services.
- Reduced financial losses from downtime and attacks.
- Cost-effective security with automated detection and mitigation.
- Efficient resource utilization, contributing to environmental sustainability.

Hexagon

RESEARCH AND REFERENCES

SMART INDIA HACKATHON 2024

- Naresh Kumar and Shalini Sharma, "Study of Intrusion Detection System for DDoS Attacks in Cloud Computing", *IEEE*, 2013, ISBN 978-1-4673-5999-3/13.
- Krishan Kumar, A.L Sangal and Abhinav Bhandari, "Traceback Techniques against DDOS Attacks: A Comprehensive Review", International Conference on Computer and Communication Technology(ICCCT), 2011.
- A. John and T Sivakumar, "DDoS: Survey of Traceback Methods", *International Journal of Recent Trends in Engineering*, vol. 1, no. 2, May 2009.
- Sujatha Sivabalan and P J Radcliffe, "A Novel Framework to Detect and Block DDoS Attack at the Application Layer", *IEEE*, 2013.
- Ahmad Sanmorino and Setiadi Yazid, "DDoS Attack Detection Method and Mitigation Using Pattern of the Flow", *International Conference of Information and Communication Technology (ICoICT)*, 2013.
- Arjun Raj Kumar and P. S. Selvakumar, "Distributed Denial-of-Service (DDoS) Threat in Collaborative Environment - A Survey on DDoS Attack Tools and Traceback Mechanisms", *IEEE International Advance Computing Conference (IACC)*, 2009.
- Yuan Tao and Shui Yu, "DDoS Attack Detection at Local Area Networks Using Information Theoretical Metrics", *IEEE Computer Society*, 2013.
- M. Baskar, T. Gnanasekaran and S. Saravanan, "Adaptive IP traceback mechanism for Detecting Low rate DDoS attacks", *IEEE(ICE-CNN)*, 2013.
- P Jayashree and K.S. Easwarakumar, "A Proactive Statistical Defense Solution for DDOS Attacks in Active Networks", First International Conference on Emerging Trends in Engineering and Technology (IEEE), 2008.
- Ritu Maheshwari, C. Rama Krishna and M. Sridhar Brahma, "Defending Network System against IP Spoofing based Distributed DoS attacks using DPHCFRTT Packet and Challenges", Intelligent Computing Techniques(ICICT), 2014.
- Martin Vizv ary and Jan Vykopal, "Future of DDoS Attacks Mitigation in Software Defined Networks", IEEE, 2014.

Hexagon

SMART INDIA HACKATHON 2024

Team Member Details

Team Leader Name: Nandayala Naveen Reddy **VTU 20906**

Branch : B.Tech Stream : CSD Year: IV

Team Member 1 Name: Sakamuri Aditya Naidu **VTU 19946**

Branch : B.Tech Stream : CSD Year: IV

Team Member 2 Name: Bandi Anod Kumar Reddy **VTU 20428**

Branch : B.Tech Stream : CSD Year: IV

Team Member 3 Name: Edda Rama Krishna Reddy **VTU20745**

Branch : B.Tech Stream : CSE Year: IV

Team Member 4 Name:

Branch : B.Tech Stream : CSD Year: IV

Team Member 5 Name:

Branch : B.Tech Stream : CSD Year: IV