SILVER OAK UNIVERSITY
EDUCATION TO INNOVATION

College of Technology (01)

Silver oka College of Engineering and Technology

Bachelor of Technology

Department of Computer SCience and Engineering Cyber Security (007)

DDOS PROTECTION SYSTEM FOR CLOUD: ARCHITECTURE & TOOLS

Group Members:

- Rohit N. Kandpal
- Veeraryan Odhavia
- Rushi Monpara
- Ganesh Prajapati

Internal Faculty Guide:

A/Prof. Shreyas Raybole

SILVER OAK UNIVERSITY
EDUCATION TO INNOVATION

CYBER SECURITY

OUTLINE

- Abstract
- Introduction
- Literature Survey/Research
- Proposed Work
- Diagram(UML)/Wireframe
- Worked carried out till date(Table format)
- Timeline Chart(Gantt Chart)
- Future Work
- Conclusion
- References

ABSTRACT

- This project focuses on designing a DDoS protection system specifically tailored for Indian government websites, which have been identified as highly vulnerable to cyberattacks.

- DDoS attacks, which overwhelm systems with excessive traffic, can severely impact the availability of essential public services provided by these websites. By leveraging cloud-based infrastructure, such as AWS EC2 and AWS Shield, this system provides a scalable and robust defense mechanism.

- It includes a web-based dashboard for real-time traffic monitoring, attack detection, and automated response mechanisms like rate limiting and IP blacklisting. The system is designed to safeguard critical public services, ensuring that government websites remain operational even during high-volume attacks.

- It aims to enhance India's overall cybersecurity framework, providing a long-term, scalable solution to protect sensitive government data and services from cyber threats.

INTRODUCTION

- This presentation focuses on a crucial issue affecting Indian government websites: their vulnerability to Distributed Denial of Service (DDoS) attacks.
- These attacks, which flood websites with excessive traffic, can cause significant disruptions, rendering government services inaccessible to citizens.
- Given the increasing reliance on digital platforms for public services, such disruptions can have widespread consequences, including delays in accessing critical services, breaches of sensitive information, and a general loss of trust in government systems.
- The goal of this project is to develop a scalable, cloud-based DDoS protection system specifically designed for Indian government websites. The system will offer: Less Downtime, Automated responses, and Cloud-based Scaling.

LITERATURE SURVEY/RESEARCH

DDoS Attacks on Indian Gov Websites

Government websites in India are vulnerable to DDoS attacks, which disrupt critical public services, highlighting the urgent need for advanced cybersecurity solutions.

Cloud-Based Defense Solutions

Cloud platforms like AWS Shield offer scalable protection, filtering malicious traffic before it reaches government servers, ensuring continuous service availability during DDoS attacks.

Botnet Identification in DDoS Attacks

Identifying botnets, which are responsible for sending large volumes of traffic, is key to mitigating DDoS attacks and preventing future occurrences by blocking their sources.

PROPOSED WORK

- **Real-time Traffic Monitoring:** Continuous monitoring of incoming traffic to identify potential threats and anomalies, including volumetric and protocol attacks.

- **Anomaly Detection & Alerting:** The system will identify unusual traffic patterns, such as sudden spikes or traffic from known malicious IP addresses, and trigger alerts.

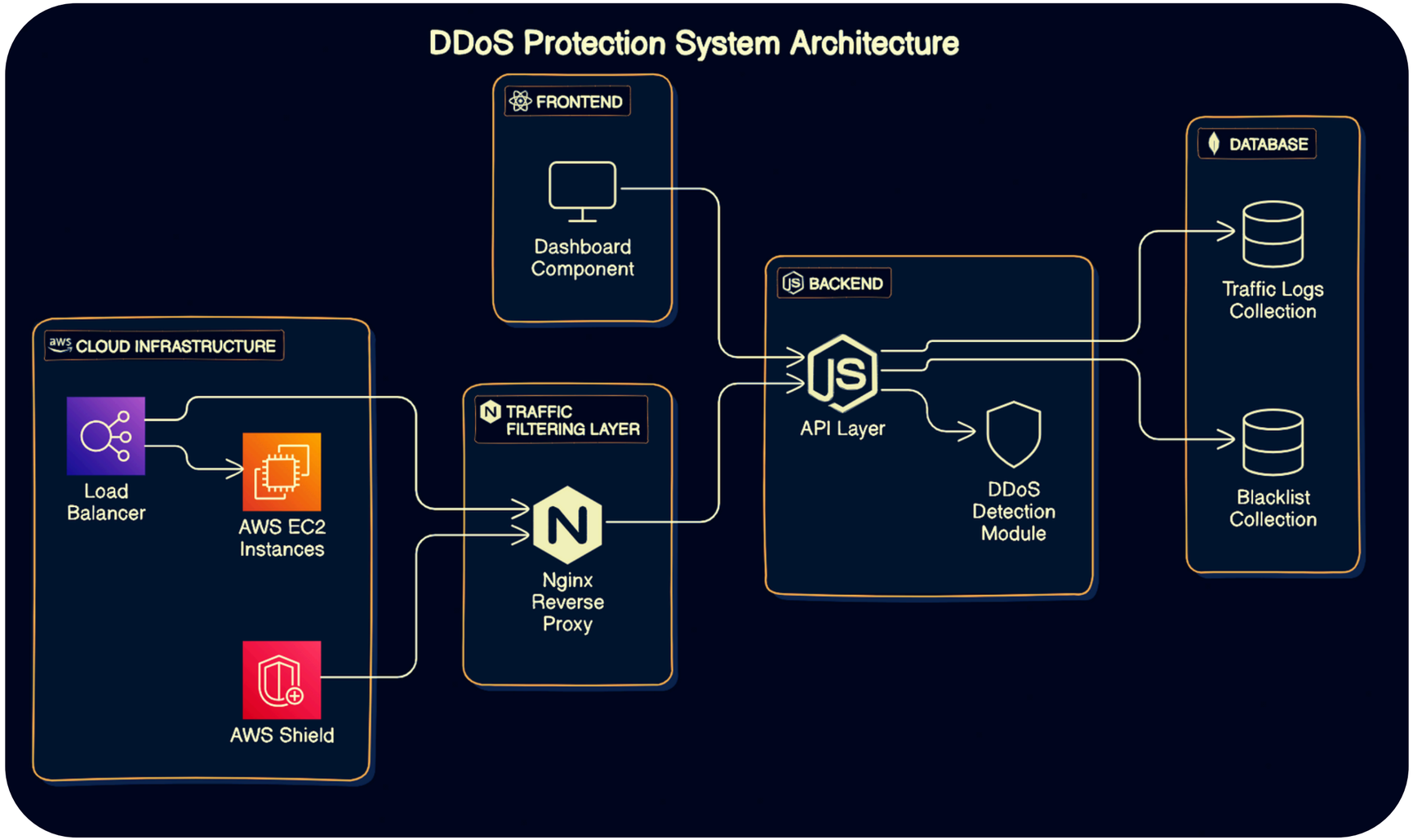
- **Automated Response Mechanisms:** The system will implement multiple layers of defense, including:

  - Rate Limiting: Automatically limiting the number of requests per second from a single IP address to prevent overload.

  - IP Blacklisting: Blocking traffic from IPs identified as malicious by the detection algorithm.

  - Scaling & Load Balancing: Automatically launching new instances of the application to handle legitimate traffic during a DDoS attack, ensuring continued service availability.

UML DIAGRAM


DDoS Protection System Architecture
FRONTEND
Dashboard Component
DATABASE
Traffic Logs Collection
BACKEND
API Layer
DDoS Detection Module
CLOUD INFRASTRUCTURE
Load Balancer
AWS EC2 Instances
AWS Shield
TRAFFIC FILTERING LAYER
Nginx Reverse Proxy
Blacklist Collection

WORK CARRIED OUT TILL DATE

Week	Task	Status
1	Problem Selection	Completed
2	Research and Requirement Gathering	Completed
3	Technology Selection	Completed
4	Architecture Creation	Completed
5	Project Build	In Progress

FUTURE WORK

- Moving forward, the system will be enhanced with machine learning models for better detection of complex attack patterns, including zero-day DDoS attacks.

- In future, an advance alerting system would be implemented which will sent an alert to all website managing people about the attack in real-time. All data about the downtimes, culprit Ip Addresses, etc.

- Additional plans include integrating AWS WAF (Web Application Firewall) for further protection and automating the process of updating the IP blacklist using known malicious IP databases.

CONCLUSION

- In conclusion, this DDoS Protection System project demonstrates a foundational approach to safeguarding web applications against potential attacks. By implementing traffic logging and IP blocking mechanisms, the project effectively identifies and mitigates suspicious activity, ensuring website availability and reliability. The use of the MERN stack, combined with MongoDB for data storage, allows for seamless integration and efficient handling of requests.

- Additionally, the project highlights the importance of continuous improvement through testing and iterative development. As the system evolves, further enhancements, such as an alerting system and user interface for monitoring, can be incorporated to provide a comprehensive solution for real-world applications. Overall, this project lays the groundwork for a more resilient web infrastructure.

THANK YOU