iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

MITIGATING DDOS ATTACKS USING RANDOM SHUFFLING GREEDY ALGORITHM: A DYNAMIC PROXY-BASED DEFENSE APPROACH

Mrs. M. Sharwani
Assistant Professor, Department of Information Technology,
Vidya Jyothi Institute of Technology, Hyderabad, India

N. Shiva Prasad, Thallapelly Rithvik, V. Naga Vignesh, K. Vinay Kumar
Students, Department of Information Technology,
Vidya Jyothi Institute of Technology, Hyderabad, India

ABSTRACT
Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks continue to be a major threat to cybersecurity, disrupting network services and causing significant downtime. This study proposes a dynamic defense mechanism using a Random Shuffling Greedy Algorithm (RSGA) to counter DDoS attacks. By assigning client requests to proxy servers in a randomized manner, the system introduces unpredictability and effectively hides the application server from attackers. This Moving Target Defense (MTD) strategy ensures improved scalability, real-time attack detection, and resilience, while maintaining uninterrupted services for legitimate users.

INTRODUCTION
With the increase in online services and cloud infrastructure, DDoS attacks have become more frequent and sophisticated. Attackers flood servers with malicious requests, making them unavailable to genuine users. Existing static methods like IP blacklisting, rate limiting, and firewalls often fail to withstand distributed attacks or insider threats. A dynamic solution is required to enhance defense capabilities.

LITERATURE SURVEY
[1] Zhang, Y., Liu, P., & Wang, H. (2020). A Comprehensive Study on DDoS Mitigation Strategies. IEEE TNSM.
[2] Xia, W., et al. (2021). ML Approaches for Detecting DDoS Attacks. IEEE Access.
[3] Jafarian, M. H., et al. (2019). MTD-Based IP Randomization. IEEE Security & Privacy.
[4] Sharmeen, A., et al. (2022). Dynamic Proxy-Based Defense for DDoS. IEEE TDSC.
[5] Zhang, Y., et al. (2022). Adaptive Proxy Allocation using RSGA. ResearchGate.
[6] Sharma, A., et al. (2024). Advancements in Detecting DDoS Attacks. JNCA.
[7] Al-Fuqaha, M., et al. (2023). Detection in IoT-Enabled Networks. JSAN.

PROPOSED SYSTEM
The system comprises four components: Client, Authentication Server, Proxy Servers, and Application Server. The client uploads files via a GUI. The Authentication Server assigns proxies using RSGA. Proxy Servers evaluate request size and drop malicious ones. Valid requests are forwarded to the Application Server for processing. Graphical logs and real-time feedback are presented to the user. This layered structure prevents attackers from identifying the application server.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

METHODOLOGY

The architecture is implemented in Python using Tkinter and socket programming. The modules include:

- Client Module: Uploads files and interacts with the Authentication Server.
- Authentication Server: Randomly assigns proxy using RSGA.
- Proxy Servers (Proxy1 & Proxy2): Detect and filter out large file requests.
- Application Server: Receives validated files and stores them. Data flow is tracked and visualized using Matplotlib.

EXPERIMENTAL RESULTS

The system was tested with normal and oversized files. Proxy Servers successfully blocked suspected DDoS attempts. Logs confirmed randomized proxy assignments. The graph interface in the client GUI visually indicated attacks and traffic load. The Application Server only received legitimate requests, confirming the system's efficiency.

CONCLUSION AND FUTURE WORK

This project demonstrates that dynamic proxy allocation using RSGA enhances DdoS defense without heavy computational overhead. The modular implementation ensures easy scalability and future upgrades. Future work includes integrating AI for adaptive learning, supporting encrypted HTTPS uploads, and deploying in cloud-based environments.

REFERENCES

1. Zhang, Y., Liu, P., & Wang, H. (2020). A Comprehensive Study on DDoS Mitigation Strategies. IEEE TNSM.
2. Xia, W., et al. (2021). ML Approaches for Detecting DDoS Attacks. IEEE Access.
3. Jafarian, M. H., et al. (2019). MTD-Based IP Randomization. IEEE Security & Privacy.
4. Sharmeen, A., et al. (2022). Dynamic Proxy-Based Defense for DDoS. IEEE TDSC.
5. Zhang, Y., et al. (2022). Adaptive Proxy Allocation using RSGA. ResearchGate.
6. Sharma, A., et al. (2024). Advancements in Detecting DDoS Attacks. JNCA.
7. Al-Fuqaha, M., et al. (2023). Detection in IoT-Enabled Networks. JSAN.