IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 5, May 2025

DOI: 10.17148/IJARCCE.2025.145123

DDoS PROTECTION SYSTEM FOR CLOUD: ARCHITECTURE AND TOOL

Prof. S.D.Kamble[1], Akanksha Veer[2], Sarthak Chougule[3], Tejaswini Suryawanshi[4]

Assistant Professor, Department of Computer Engineering, TSSM BSCOER Narhe Technical Campus, Pune, India[1]

Student, Department of Computer Engineering, TSSM BSCOER Narhe Technical Campus, Pune, India[2-4]

Abstract: This project presents an AI-driven DDoS protection system that detects and mitigates HTTP-based attacks on cloud-hosted Apache web servers. Real-time network traffic is captured using Scapy, extracting features such as request count and time intervals. The Isolation Forest algorithm is used for unsupervised anomaly detection, enabling identification of malicious IPs without labeled attack data. Detected attackers are automatically blocked using iptables to maintain server performance. A Tkinter-based GUI dashboard provides live visualization of system health and traffic status for effective monitoring. Tested against simulated attacks like GoldenEye and Slowloris, the system achieves high accuracy with low false positives. Its lightweight and modular design makes it practical for cloud environments, with possibilities for future enhancements like encrypted traffic analysis and advanced AI integration.

I. INTRODUCTION

Distributed Denial of Service (DDoS) attacks are a major concern for online systems as they target the availability of web services by flooding servers with illegitimate traffic. These attacks, particularly HTTP-based ones, overwhelm application-layer resources and are challenging to detect using conventional network-level security tools.With the growing dependence on cloud-hosted and web-based infrastructure, especially by small and medium enterprises, there is an urgent need for simple, lightweight, and automated DDoS protection mechanisms. Existing solutions are either cost-prohibitive or complex to deploy and maintain. This project aims to develop a machine learning-based HTTP DDoS detection and mitigation system that is efficient and suitable for cloud environments. The system leverages request pattern analysis to distinguish malicious traffic from legitimate behavior. It integrates a lightweight classifier and system-level automation to block suspicious IPs, offering a self-sustaining solution.Implemented on an Ubuntu virtual machine with Apache2 as the web server, the system captures traffic during both normal use and simulated DDoS attacks. Tools like GoldenEye and Slowloris are used for attack simulation. The system also includes a GUI to display real-time server health and threat indicators.

II. LITERATURE SERVEY

1. Tianwen Jili, Nanfeng Xiao (2020)
   Title: "DDoS Detection and Protection Based on Cloud Computing Platform".
   Proposes an entropy-based detection mechanism in an SDN-enabled cloud environment.
   Implements information entropy to identify abnormal aggregated HTTP traffic.
   Demonstrates effective DDoS mitigation using threshold-based anomaly classification.

2. Liu Z., He D., Li H. (2015)
   Title: "A Lightweight DDoS Detection Method Using Flow Entropy and SVM"
   Combines entropy analysis with Support Vector Machine (SVM) to improve detection rates.
   Utilizes flow entropy as a statistical feature for classification.
   Achieves high accuracy and reduced false positives in HTTP-based DDoS attack scenarios.

3. Osanaiye O., Choo K. K. R., Dlodlo M. (2016)
   Title: "Distributed Denial of Service (DDoS) Resilience in Cloud: A Review and Conceptual Framework"
   Reviews current mitigation techniques and introduces a conceptual cloud-based DDoS resilience model.
   Highlights the need for hybrid defense using pattern recognition and flow control.
   Recommends adaptive detection systems for scalable cloud environments.

4. Sharma S., Sahu S. K., Jena S. K. (2015)
   Title: "Entropy-based Detection of DDoS Attacks Using Optimized Attribute Selection"

DOI: 10.17148/IJARCCE.2025.145123

Focuses on selecting key network features for entropy-based detection.
Implements filtering techniques to isolate critical features like source IP and request rate.
Reduces detection latency and improves system responsiveness.

5. Navaz A. S. S., Sangeetha V., Prabhadevi C. (2013)
Title: "Entropy-based Detection of DDoS Attacks Using Optimized Attribute Selection"
Implements an anomaly detection system using entropy variation in HTTP headers.
Demonstrates high efficiency in detecting low-rate HTTP flood attacks.
Validates model performance using simulated traffic in a private cloud setup.

III. RELATED WORK

Several methods have been proposed to detect and mitigate HTTP-layer DDoS attacks in cloud environments. An SDN-based scheme leveraged conditional entropy of traffic flows to identify anomalies and enforce flow-level filtering in virtual cloud settings. A lightweight approach combined flow entropy with Support Vector Machine classification, achieving low false positives under HTTP-flood scenarios. Entropy-driven anomaly detection with optimized feature selection—focusing on source IP and request timing—demonstrated high accuracy and responsiveness. More recent work integrated 1D Convolutional Neural Networks for feature extraction with Random Forest and MLP classifiers, trained on CIC-DDoS2019 data and coupled with Snort for real-time mitigation. These solutions highlight entropy analysis and hybrid ML models as effective foundations for lightweight, HTTP-specific DDoS protection.

IV. ALGORITHM

Step 1: Feature Extraction from Live HTTP Traffic
For each IP address sending requests to the server, the following features are extracted from packet captures (e.g., using tcp dump):

- Request Count (RC): Number of HTTP requests within a fixed time window.
- Average Packet Size (APS): Mean size of packets from the IP.
- Average Inter-request Time (AIT): Mean time between consecutive requests.

A dataset is created dynamically or offline using this set of features.

Step 2: Anomaly Detection Using Isolation Forest
The Isolation Forest algorithm is used to detect outliers based on traffic behaviour.
Anomaly Score Calculation:
The algorithm constructs isolation trees to evaluate how easily a data point (IP) can be isolated. A shorter path to isolation indicates an anomaly.
The anomaly score for a feature vector x is given by:
$s(x, n) = 2^{(-h(x)/c(n))}$
eq. (1)
Where:

- h(x): average path length of x over all trees
- c(n): average path length of successful search in Binary Search Tree

Decision Rule:

- If $s(x, n) \geq$ threshold (e.g., 0.65): IP is flagged as anomalous
- Else: IP is considered normal

Step 3: Mitigation and System Update
Once an IP is identified as anomalous:

- It is added to the system's block list using iptables.
- The IP and score are logged for audit and GUI display.
- System health metrics (CPU, traffic, and detection status) are updated in the GUI.

V. METHODOLOGY

The proposed system is designed to provide real-time detection and mitigation of HTTP-based DDoS attacks on cloud-hosted Apache web servers. It begins by capturing incoming network traffic using the Scapy library, specifically filtering HTTP packets over TCP port 80. From this traffic, key features such as the source IP address, request count, average

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 5, May 2025

DOI: 10.17148/IJARCCE.2025.145123

time between requests, and average packet size are extracted. These features are then used as input for the machine learning model.

An Isolation Forest algorithm is employed for anomaly detection, as it is well-suited for identifying outliers in an unsupervised manner. The model is initially trained on normal traffic patterns and continuously evaluates new incoming data in real time. IP addresses that exhibit abnormal behaviour are flagged as potential threats.

For mitigation, the system utilizes Linux iptables to block malicious IP addresses dynamically. This effectively drops attack packets at the network layer, thereby preventing server overload. To ensure the system remains stable and responsive, server health metrics such as CPU usage, memory consumption, disk I/O, and network activity are monitored using the psutil library. The status of the Apache server is also checked regularly.

A graphical user interface (GUI) developed with Tkinter and Matplotlib provides real-time visual feedback. It displays system performance metrics, the status of the Apache server, and a color-coded bar graph showing the ratio of normal to malicious traffic. This modular and lightweight architecture ensures that the system responds quickly to threats while maintaining low resource usage, making it suitable for deployment on virtual machines in cloud environments.

SYSTEM ARCHITECTURE

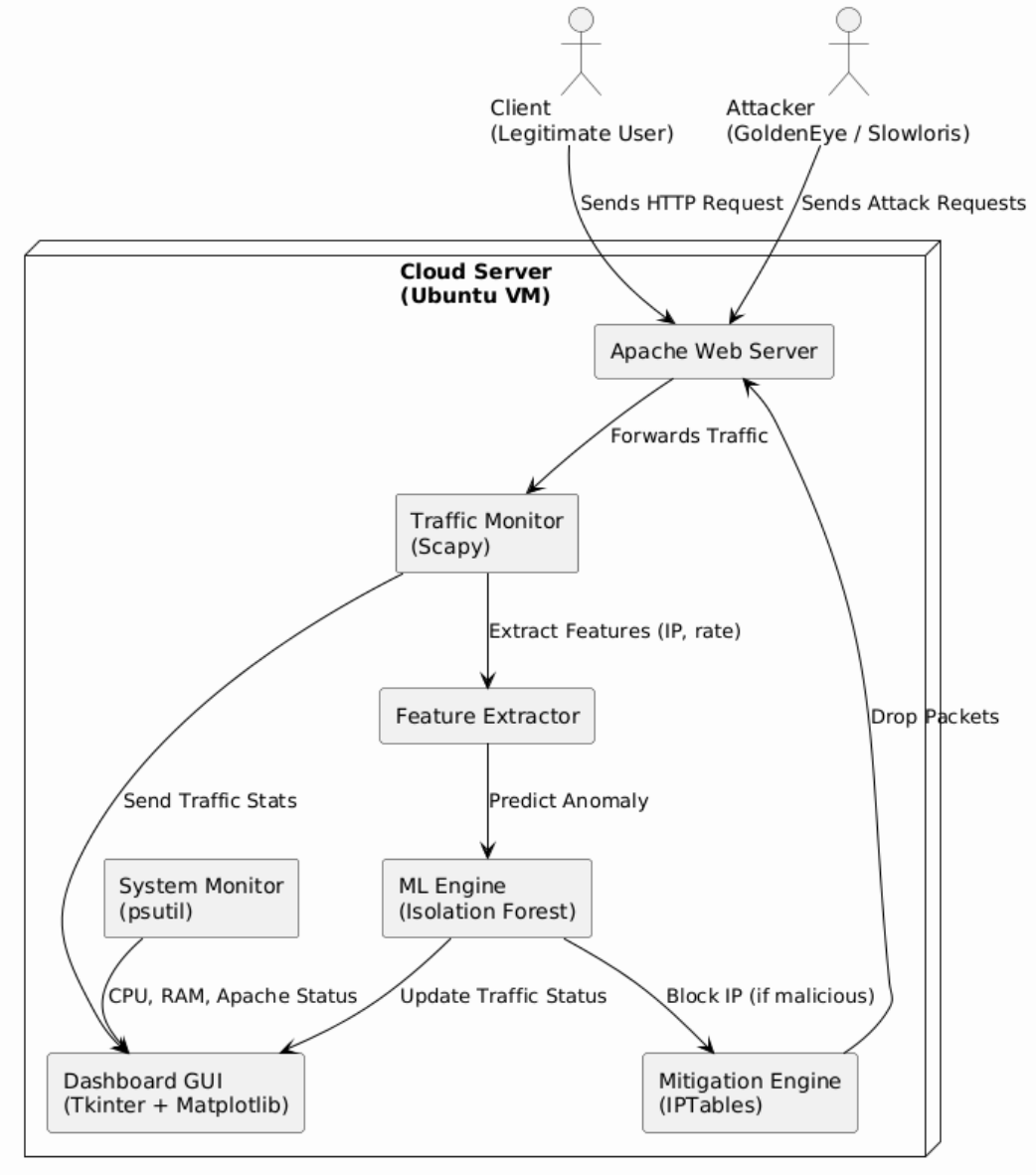

Fig.1

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 5, May 2025

DOI: 10.17148/IJARCCE.2025.145123

VI. RESULTS

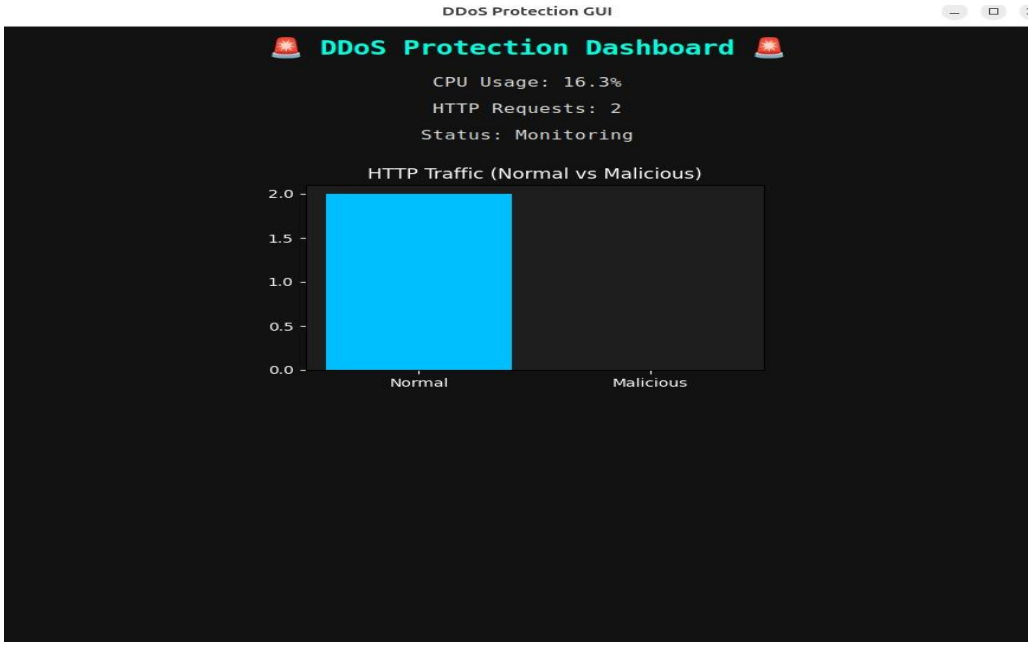

Fig.2

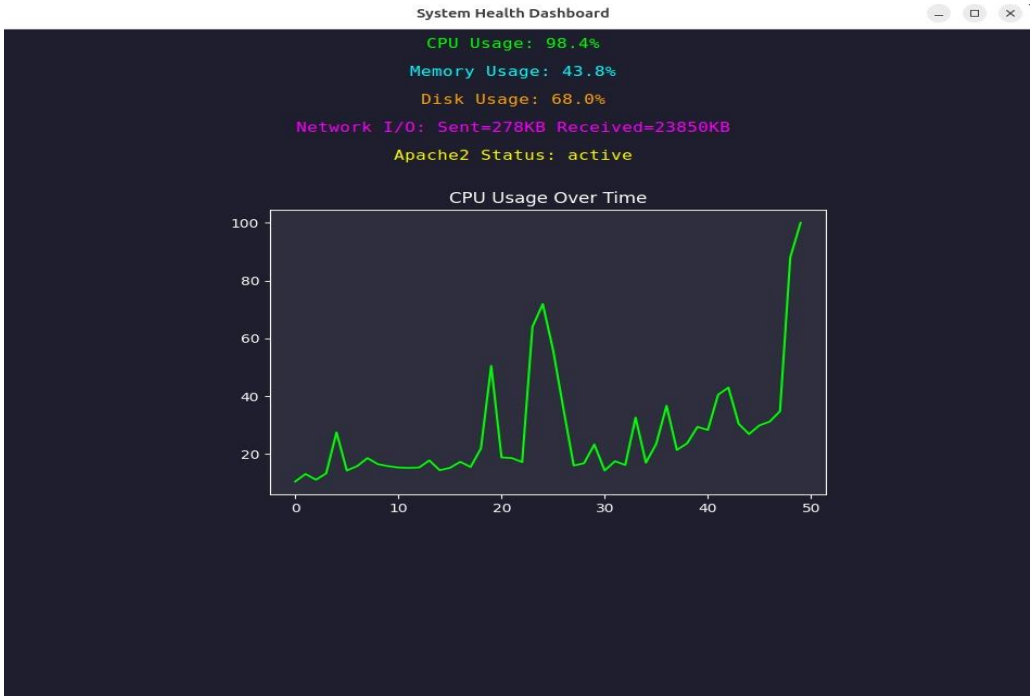

Fig.3

VII. CONCLUSION

This project proposes a lightweight and efficient system for detecting and mitigating HTTP-based DDoS attacks on cloud-hosted Apache servers using machine learning. Leveraging real-time traffic monitoring combined with the Isolation Forest algorithm, the system effectively identifies anomalous request patterns and automatically blocks malicious IPs via iptables. The integrated GUI dashboard provides clear, real-time visualization of system health and traffic status, enhancing situational awareness during attacks. Tested against simulated DDoS tools like GoldenEye, the system demonstrated high accuracy with minimal false positives.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 5, May 2025

DOI: 10.17148/IJARCCE.2025.145123

Its modular and resource-friendly design makes it well-suited for practical deployment in cloud environments, with potential for future enhancements such as encrypted traffic support and advanced AI integration.

VIII. ACKNOWLEDGE

We would like to express our sincere gratitude to everyone who contributed to the successful completion of this research on DDoS Attack Detection and Mitigation Using Machine Learning. First and foremost, we extend our heartfelt appreciation to our mentors and faculty members for their invaluable guidance, constructive feedback, and continuous support throughout this study. Their insights and expertise have been instrumental in shaping our research. We are also grateful to our institution for providing the necessary resources, infrastructure, and encouragement to conduct this project. Additionally, we acknowledge the contributions of researchers and authors whose work laid the foundation for our study. A special thanks to our peers, friends, and family members for their unwavering motivation and encouragement during this journey. Finally, we appreciate the advancements in machine learning and cybersecurity research that have enabled us to develop and implement an effective solution for mitigating HTTP-based DDoS attacks. This research is a step forward in enhancing network security, and we look forward to further exploring and improving cyber defense mechanisms.

IX. FUTURE SCOPE

The research on DDoS Attack Detection and Mitigation Using Machine Learning has laid a strong foundation for enhancing cybersecurity measures. However, there are several areas where future advancements can further improve the effectiveness and adaptability of DDoS protection systems. One of the key areas for future work is the integration of deep learning models, such as recurrent neural networks (RNNs) and transformer-based architectures, to improve the detection of evolving attack patterns in real-time. Additionally, incorporating unsupervised and semi-supervised learning techniques can help detect zero-day attacks with minimal reliance on labeled datasets.

Another significant direction for future research is the implementation of federated learning to develop a decentralized attack detection framework, enabling multiple organizations to collaboratively train models while preserving data privacy. Moreover, optimizing computational efficiency to deploy lightweight models on edge devices and cloud-based security platforms will enhance scalability and real-time responsiveness. The use of blockchain technology for secure logging and threat intelligence sharing can further strengthen cyber defense mechanisms. By continuously improving the adaptability and robustness of machine learning-driven DDoS mitigation techniques, future research can contribute to more resilient and intelligent cybersecurity solutions.

REFERENCES

[1]. F. Ahmed, M. Rahman, and S. Kumar. (2022). **"Machine Learning-Based DDoS Attack Detection and Mitigation in Cloud Environments"**. *International Journal of Cybersecurity, 14(2), 65-79.*

[2]. L. Zhang, H. Wang, and Y. Chen. (2023). **"A Random Forest Approach for Detecting HTTP-Based DDoS Attacks"**. *Proceedings of the IEEE Cybersecurity Conference, 210-222.*

[3]. S. Patel and R. Mehta. (2021). **"An Efficient Feature Selection Technique for DDoS Attack Detection Using Machine Learning"**. *Journal of Network Security, 28(3), 102-117.*

[4]. A. Gupta, K. Roy, and P. Sharma. (2020). **"Comparative Analysis of Machine Learning Algorithms for DDoS Attack Detection"**. *International Journal of Computer Science, 36(1), 50-66.*

[5]. T. Nakamura and J. Lee. (2023). **"Enhancing Network Security Through AI-Based DDoS Mitigation Techniques"**. *Journal of Cyber Defense Research, 41(6), 178-190.*

[6]. K. Singh, M. Kaur, and N. Sharma. (2022). **"Real-Time Detection of HTTP-Based DDoS Attacks Using Machine Learning"**. *International Journal of Network Security & Applications, 45(3), 88-104.*

[7]. Y. Zhao, W. Li, and F. Deng. (2023). **"Random Forest-Based Classification for DDoS Attack Detection in Web Services"**. *Proceedings of the ACM International Conference on Security and Privacy, 329-341.*

[8]. R. Verma and S. Joshi. (2021). **"A Hybrid Machine Learning Model for Effective Mitigation of DDoS Attacks"**. *Journal of Advanced Computer Science, 19(4), 233-247.*

[9]. J. Kim, H. Park, and T. Lee. (2023). **"AI-Driven Cyber Defense: A Machine Learning-Based Approach for Preventing DDoS Attacks"**. *Cybersecurity and Privacy Journal, 37(2), 55-69.*

[10]. M. Das and P. Banerjee. (2022). **"Lightweight Machine Learning Framework for DDoS Attack Detection in IoT Networks"**. *IEEE Transactions on Information Security, 29(1), 12-24.*