2025 5th Asian Conference on Innovation in Technology (ASIANCON)
Pune, India. Aug 22-23, 2025

DDoS Protection Using a Honeynet Implementation with Offensive Capabilities

Sonali Patil
Department of Computer Engineering
Pimpri Chinchwad College of Engineering
Nigdi, Pune - 411044, India
sonali.patil@pccoepune.org

Nikhil Pattewar
Department of Computer Engineering
Pimpri Chinchwad College of Engineering
Nigdi, Pune - 411044, India
nikhil.pattewar22@pccoepune.org

Swarnim Bhadale
Department of Computer Engineering
Pimpri Chinchwad College of Engineering
Nigdi, Pune - 411044, India
swarnim.bhadale22@pccoepune.org

Ramiz Shaikh,
Department of Computer Engineering
Pimpri Chinchwad College of Engineering
Nigdi, Pune - 411044, India
ramiz.shaikh23@pccoepune.org

Bhargav Mule,
Department of Computer Engineering
Pimpri Chinchwad College of Engineering
Nigdi, Pune - 411044, India
bhargav.mule22@pccoepune.org

2025 5th Asian Conference on Innovation in Technology (ASIANCON) | 979-8-3503-5699-1/25/$31.00 ©2025 IEEE | DOI: 10.1109/ASIANCON66527.2025.11280733

***Abstract* – Distributed Denial of Service (DDoS) attacks represent a persistent and evolving threat to online services, aiming to exhaust resources and disrupt availability. This research paper proposes a novel approach to DDoS protection through the strategic implementation of a honeynet. By deploying a network of decoy systems designed to attract and capture malicious traffic, a honeynet provides a controlled environment for the in-depth analysis of DDoS attack methodologies and attacker behavior. This capability allows for the real-time collection of threat intelligence regarding emerging attack vectors, tools, and techniques. Beyond traditional honeynet functionalities of detection and mitigation through traffic diversion and blacklisting, this paper explores the integration of 'offensive capabilities'. These capabilities leverage the insights gained from analyzing attacks within the honeynet to inform proactive defense strategies, potentially disrupting attacker infrastructure or preemptively neutralizing threats. This research contributes to advancing the field of DDoS defense by presenting an enhanced honeynet-based security framework that moves beyond reactive measures towards a more dynamic and intelligent response to the evolving DDoS threat landscape.**

Keywords: DDoS attacks, honeynet, DDoS protection, threat intelligence, offensive capabilities, attacker behavior, malicious activity, defense strategies.

I. INTRODUCTION

The escalating prevalence and sophistication of Distributed Denial of Service (DDoS) attacks represent a significant and persistent threat to the availability and reliability of online services and network infrastructure [1], [12], [13], [19]. These malicious attempts to overwhelm target systems with a flood of traffic can lead to severe disruptions, financial losses, and damage to reputation [5], [21], [32]. As networks evolve with the adoption of technologies like cloud computing [15], [20], Software-Defined Networking (SDN) [7], [11], [12], [19], [24], [30], and the proliferation of Internet of Things (IoT) devices [3], [6], [30], the attack surface expands, and the need for more adaptive and effective defense mechanisms becomes increasingly critical [12], [19], [21], [22]. The relative ease with which attackers can access and utilize DDoS attack tools further exacerbates this challenge [13], [17], [29].

Traditional security measures, while essential, often fall short in adequately addressing the dynamic nature and sheer volume of modern DDoS attacks [12], [21]. Intrusion Detection Systems (IDS) and mitigation techniques frequently focus on identifying known attack signatures or anomalies in traffic patterns [10], [36], but may struggle with novel attack vectors, including Low-Rate DDoS (LR-DDoS) attacks designed to evade detection [14], [18], [21], [24], [26] and Memory Denial of Service (M-DoS) attacks targeting resource exhaustion in cloud environments [15]. Furthermore, many existing defense strategies are largely reactive, responding to attacks once they have already commenced [5], rather than proactively preventing or significantly mitigating their impact at an early stage [17], [22].

This research proposes a novel approach to DDoS protection through the implementation of a honeynet architecture integrated with offensive capabilities. By strategically deploying decoy systems (honeypots) designed to attract and capture malicious DDoS traffic [2], [29], [32], [38], valuable insights into attacker behavior, tools, and techniques can be gathered in real time [29], [38], [41]. Leveraging this enriched cyber threat intelligence, the proposed solution aims to go beyond traditional reactive defense mechanisms by incorporating proactive measures and carefully considered offensive actions to potentially disrupt attacker infrastructure or mitigate the attack closer to its source [18], [41]. This integration of deception and active defense seeks to create a more resilient and adaptive security posture against the evolving DDoS threat landscape.

A. Problem Statement

Distributed Denial of Service (DDoS) attacks have become a major threat to internet availability and security over the past few decades. These attacks aim to disrupt or halt the targeted machine or network, rendering it inaccessible to legitimate users by either exhausting network bandwidth or consuming host resources. The increasing sophistication and frequency of DDoS attacks pose significant challenges to online services and infrastructure. Contemporary mobile networks, while offering advanced services, also face heightened vulnerability at the radio interface, a primary access medium, including DDoS attacks leveraging the IP protocol stack. Moreover, the rise of cloud computing

environments, connected applications, and Internet of Things (IoT) devices has progressively increased the amount of data traversing networks, making them attractive targets for DDoS attacks.

Traditional network security measures, such as firewalls, are designed to keep attackers out, but they often struggle to effectively detect and mitigate the diverse and evolving tactics employed in DDoS attacks. While Intrusion Detection Systems (IDS) aim to tackle security issues, especially those related to ICMPv6-based DoS and DDoS attacks, classifying them as anomaly-based or signature-based may lack the detailed view needed for approaches like Machine Learning (ML) techniques. Furthermore, many existing DDoS detection and mitigation methods often focus on specific attack types, leaving them potentially vulnerable to other forms of attack. The ease of access to freely available DDoS attack tools can also exacerbate the frequency and severity of these attacks, allowing individuals with limited technical expertise to launch significant attacks. The economic and reputational damage inflicted by successful DDoS attacks underscores the urgent need for more robust and adaptive defense mechanisms. Even in Software-Defined Networking (SDN), which offers advantages like centralized control, DDoS attacks remain a critical security challenge, affecting network performance and availability by targeting the controller, data plane devices, or northbound APIs. The persistent challenge of DDoS attacks, including Low-Rate DDoS (LR-DDoS) attacks that are particularly difficult to detect, highlights the limitations of current mitigation strategies. Memory Denial of Service (M-DoS) attacks, which target memory resources, further complicate the threat landscape, especially in cloud environments where resources are shared.

B. *Gaps Identified*

Several gaps exist in the current landscape of DDoS detection and mitigation techniques. Many studies have focused on single detection methods, with few utilizing multiple or integrated approaches to address DDoS threats comprehensively across different network layers. Existing surveys on DDoS detection in SDN sometimes lack a comprehensive taxonomy to guide readers through the complexities of DDoS attack types and detection methods tailored to SDN environments. Some reviews focus on specific environments like cloud computing or IoT scenarios without providing a broader perspective. Furthermore, there is a lack of in-depth discussions and actionable insights in some surveys, leaving readers without a clear understanding of the practical applicability of each method within an SDN context.

While numerous Machine Learning (ML) and Deep Learning (DL) techniques have been proposed for DDoS detection, many existing methods primarily concentrate on recognizing attack patterns and types rather than the specific tools used to launch these attacks. The adaptability of ML and DL models to evolving attack patterns in real-time continues to pose challenges. For ICMPv6-based DDoS attacks, there is a lack of review papers specifically focused on IDSs based on ML techniques. In the realm of LR-DDoS attacks, existing studies need to be updated with new information on emerging attacks, defense mechanisms, and classifications. Moreover, some proposed detection methods may require more technology to determine thresholds and multi-element weight distribution or may be complex and inefficient due to the need to distinguish packet protocols. The detection accuracy for certain traffic types, like ICMP, can also be low in some ML-based approaches.

The application of honeypots for mitigating DDoS attacks, particularly in modern network environments like SDNs and cloud environments, while promising, still has areas that need exploration. Some research remains theoretical, with only theoretical models proposed [28]. There is a need to address the limitations of single honeypots in tackling large-scale, volume-based DDoS attacks, especially those utilizing botnets [9]. Furthermore, the integration of offensive security capabilities into DDoS defense strategies, leveraging the intelligence gathered from honeypots for proactive measures and potential counterattacks, appears to be a relatively underexplored area in the existing literature.

C. *Objectives*

The primary objectives of this research are as follows:

1. To design and implement a novel DDoS protection system based on a honeynet architecture.
2. To integrate offensive capabilities within the honeynet framework to enhance DDoS defense.\
3. To attract and divert malicious DDoS traffic to the deployed honeypots.
4. To analyze the captured attack patterns and characteristics within the honeynet environment to gather enriched cyber threat intelligence.
5. To develop strategies for proactive defense and potential counterattacks based on the intelligence gained.
6. To evaluate the effectiveness and efficiency of the proposed honeynet implementation with offensive capabilities in detecting, diverting, and potentially mitigating DDoS attacks.
7. To address some of the identified gaps in existing DDoS defense mechanisms, such as the need for more dynamic and adaptive strategies.

D. *Scope*

The scope of this research will focus on:

1. The design and implementation of a honeynet consisting of low to medium interaction honeypots capable of emulating vulnerable services and attracting a variety of DDoS attack types.
2. The integration of tools and techniques within the honeynet infrastructure to analyze captured DDoS attack traffic, identify attacker behaviors, and extract relevant threat intelligence.
3. The development of offensive capabilities that can leverage the gathered threat intelligence for proactive defense measures. This may include techniques for disrupting attacker infrastructure or preemptively blocking malicious sources while carefully considering ethical implications.
4. The evaluation of the proposed system against various types of DDoS attacks, including but not limited to flooding attacks (e.g., SYN flood, UDP flood), application-layer attacks (e.g., HTTP flood), and potentially low-rate DDoS attacks.

5. The deployment and testing of the honeynet in a simulated network environment, potentially leveraging SDN technologies like Mininet for greater flexibility and control.
6. The analysis of key performance metrics, such as the rate of malicious traffic diversion, the accuracy of threat intelligence gathering, and the effectiveness of offensive capabilities in mitigating the impact of DDoS attacks.

The research may consider the applicability of the proposed solution in various network environments, including traditional networks, Software-Defined Networks (SDNs) [12], and cloud computing environments [25], although the primary focus may be on a simulated SDN environment. The ethical and legal considerations associated with offensive security capabilities will be acknowledged and addressed throughout the research.

E. Motivation

The motivation for this research stems from the increasingly severe and sophisticated nature of Distributed Denial of Service (DDoS) attacks and the limitations of existing security measures in effectively countering them [5], [32]. The proliferation of cloud computing, SDN, and IoT devices has expanded the attack surface, making online services more vulnerable to disruptive floods of malicious traffic [27]. Furthermore, the ease of access to DDoS attack tools lowers the barrier for malicious actors, heightening the urgency for more robust defenses [13]. Traditional security systems often struggle with novel attack vectors like Low-Rate DDoS and Memory Denial of Service attacks, tending to be reactive rather than preemptive in their response [15]. Therefore, there is a compelling need to explore and develop more adaptive and proactive strategies that can not only detect and mitigate DDoS attacks but also gather valuable intelligence on attackers and potentially disrupt their operations. This research is motivated by the desire to move beyond conventional reactive defenses by integrating the deceptive capabilities of honeynets with carefully considered offensive actions, aiming to create a more resilient and effective security posture against the evolving DDoS threat landscape [41].

F. Organization of the Paper

The remainder of this paper is organized as follows: Section II provides the necessary background on DDoS attacks, honeynets, and offensive security concepts. Section III presents a detailed review of related work in DDoS detection and mitigation techniques, as well as the use of honeypots and offensive measures in cybersecurity. Section IV outlines the methodology employed in this research, including the design and architecture of the proposed honeynet with offensive capabilities. Section V describes the proposed solution in detail, elaborating on its key components and functionalities. Section VI discusses the implementation aspects of the system, including the system architecture, key functionalities, and development stack. Section VII provides a security analysis of the proposed solution. Section VIII presents the results of the experimental evaluation. Finally, the paper concludes in Section IX with a summary of the findings and directions for future research, followed by the list of references in Section X.

II. BACKGROUND

Distributed Denial of Service (DDoS) attacks pose a significant threat to the availability and security of online services by overwhelming target systems with a flood of malicious traffic from multiple sources [5]. These attacks can exhaust network bandwidth, consume server resources, and ultimately render services unavailable to legitimate users [11], [25], [29]. The increasing prevalence and sophistication of DDoS attacks necessitate the development of more effective defense mechanisms [19], [26], [32]. While traditional Denial of Service (DoS) attacks originate from a single source, DDoS attacks leverage a distributed network of compromised devices, often forming botnets, making them more challenging to detect and mitigate [9], [29]. Different types of DDoS attacks exist, targeting various layers of the network infrastructure. These include flooding attacks that aim to saturate network bandwidth [11], application-layer attacks that target specific applications and services [11], [17], protocol-based attacks that exploit weaknesses in network protocols, and resource-exhaustion attacks that consume critical resources of the target system [12]. The impact of DDoS attacks can be severe, leading to service disruptions, financial losses, and reputational damage [16], [19].

Honeypots and honeynets are valuable tools in cybersecurity that function as decoy systems designed to attract and trap malicious activity [28]. A honeypot is a single deceptive resource, while a honeynet is a network of such resources, mimicking real production systems but containing limited or no legitimate data. By attracting attackers, honeypots and honeynets allow security professionals to observe attacker behavior, analyze their tools and techniques, and gather valuable threat intelligence [9]. The interactions with honeypots can provide insights into emerging attack trends and vulnerabilities [32]. Different types of honeypots exist, ranging from low-interaction honeypots that emulate basic services to high-interaction honeypots that run full operating systems and applications, offering a more realistic target for attackers [29], [35]. The deployment of honeypots can aid in the early detection of attacks and the diversion of malicious traffic from critical assets [28], [30], [32].

Offensive capabilities, in the context of cybersecurity, refer to proactive security measures that go beyond traditional detection and prevention strategies. This can involve actively engaging with attackers to gather more information, disrupt their activities, or even proactively address vulnerabilities in their infrastructure. The concept of active defense suggests a more dynamic and adaptive approach to security, where organizations take a more assertive role in countering threats. Integrating offensive capabilities with defensive measures can potentially enhance an organization's security posture by not only identifying and mitigating attacks but also by gaining a deeper understanding of the threat actors and their methods. However, the implementation of offensive strategies requires careful consideration of ethical and legal implications [41].

The integration of a honeynet implementation with offensive capabilities presents a novel approach to DDoS protection. By deploying a honeynet to attract DDoS attacks, real-time intelligence on attack vectors and sources can be gathered. This information can then potentially be leveraged to inform and trigger offensive actions aimed at mitigating the attack or disrupting the attacker's infrastructure. This approach seeks to move beyond purely reactive defense

mechanisms by actively engaging with and potentially countering DDoS threats more comprehensively.

III. RELATED WORK

The related work in the field of DDoS protection encompasses a wide range of approaches, including various detection and mitigation techniques, the use of honeypots, and considerations for specific network environments like Software-Defined Networking (SDN) and cloud computing. Numerous studies have focused on detecting DDoS attacks using techniques such as machine learning (ML), deep learning (DL)], statistical analysis, and anomaly detection. For instance, ML algorithms like KNN SVM [15], [27], Random Forest [12], [14], and neural networks [11], [13] have been explored for traffic classification and attack identification [27]. Some research specifically addresses the challenges of Low-Rate DDoS (LR-DDoS) attacks, which are designed to evade traditional detection methods [26]. These studies propose various techniques for detecting such subtle attacks [12], [24].

Honeypots have been investigated as a means to detect and mitigate DDoS attacks by attracting and trapping malicious traffic [28], [32]. Different types of honeypots, including low-interaction and high-interaction, have been deployed to analyze attacker behavior and gather threat intelligence [29], [35]. The use of distributed virtual honeypots in Content Delivery Networks (CDNs) has also been explored for DDoS mitigation [27]. Furthermore, the integration of honeypots within specific network architectures like SDN and Industrial Internet of Things (IIoT) [3] has been studied to provide dynamic protection and analyze attacks in these unique environments. Some works propose pseudo-honeypot strategies in SDN to enhance defense against DDoS attacks [30].

The unique characteristics of Software-Defined Networking (SDN) have been leveraged for DDoS defense due to its centralized control and programmability [19]. Various SDN-based approaches for DDoS detection and mitigation have been proposed, including methods based on flow statistics, table entries, scheduling, and architectural modifications [7]. Machine learning techniques have also been widely applied for DDoS detection in SDN environments [24], [27]. Additionally, surveys have been conducted to classify and compare different DDoS mitigation techniques in SDN [7], [8], [11], highlighting their strengths, limitations, and applicability. The security challenges and countermeasures related to DDoS attacks in SDN have been a significant focus of research [19], [26].

In the context of cloud computing, the detection and mitigation of DDoS attacks are critical for ensuring the availability of cloud services [20], [27]. Research has addressed various types of DDoS attacks targeting cloud environments, including Memory DoS (M-DoS) attacks [15] and TCP flood attacks [16]. Machine learning-based detection systems have been proposed for identifying malicious traffic in the cloud [27]. The use of container-based honeypot deployments for analyzing malicious activity in cloud environments has also been explored [14], [35]. Some studies have investigated the impact of low-rate DDoS attacks on cloud auto-scaling mechanisms [21] and proposed defenses for container-based cloud environments [12].

While the sources extensively cover DDoS detection and mitigation techniques and the use of honeypots in various network contexts, there is less explicit focus on integrated solutions combining honeynets with offensive capabilities. Some papers discuss active defense strategies in general [19], and the concept of using honeypots to gather intelligence that could inform a more proactive response is implicit in their design. However, dedicated research on the systematic integration of honeynet-derived intelligence to trigger specific offensive actions against DDoS attackers is a less explored area within these sources. This suggests a potential gap that your research could address.

IV. METHODOLOGY

A. *Research Design*

This research follows an experimental and quantitative approach to demonstrate an advanced DDoS protection system using a honeynet with offensive capabilities. The study involves setting up a controlled network environment where a simulated DDoS attack is launched, and the effectiveness of the honeynet in mitigating and countering these attacks is analyzed. The research primarily focuses on real-time traffic analysis, filtering, and response mechanisms using machine learning techniques and active defense strategies.

B. *Data Collection Methods*

The data for this research is collected using real-time network monitoring and logging tools. The experimental setup includes capturing network traffic logs, attack patterns, and responses using Wireshark, which provides insights into packet flows and anomalies. Additionally, a pre-trained machine learning model is employed, which is trained on the CICDDoS2019 dataset to classify incoming requests as legitimate or malicious. The data includes features like source IP, destination IP, packet size, protocol type, and request frequency, which aid in detecting and blocking DDoS attacks.

C. *Materials & Tools*

The study is conducted using six physical machines running Ubuntu OS:

1) Attacker (10.12.2.167) – Executes DDoS attacks using Low Orbit Ion Cannon (LOIC).
2) Bot 1 (10.12.0.198) & Bot 2 (10.12.0.215) – Act as compromised machines controlled via SSH.
3) Honeypot 1 (10.12.2.97) – First line of defense, filtering traffic using iptables and running the XGBoost ML model.
4) Honeypot 2 (10.12.0.192) – Acts as a load balancer and secondary filter, utilizing HAProxy.
5) Target Machine (10.12.2.98) – Hosts the nist_clone website and receives only legitimate traffic.

D. *Experimental Setup*

The attacker machine remotely controls the two bot machines via SSH, executing LOIC-based DDoS attacks targeting Honeypot 1. The honeynet operates as follows:

1) **Honeypot 1 (Primary Filter):** Intercepts all traffic and runs the XGBoost-based ML model to classify requests. Legitimate requests are forwarded to the target machine, and Malicious requests are logged, blocked using iptables, and countered using reverse attack packets.

2) **Honeypot 2 (Load Balancer & Secondary Filter):** If traffic on Honeypot 1 exceeds a predefined threshold, requests are redirected to Honeypot 2. It applies additional filtering using the same ML model. Legitimate traffic is forwarded to the target machine.

E. Algorithms/Models

The study utilizes an XGBoost-based machine learning model trained on the CICDDoS2019 dataset. The model classifies traffic based on features such as:

- Source IP and destination IP
- Packet count and size
- Frequency of requests
- Protocol types (TCP, UDP, HTTP, etc.)
- Time intervals between requests
- The trained model, stored as xgboost_ddos_model.pkl, is deployed on both honeypots for real-time classification.

F. Evaluation Metrics

The effectiveness of the proposed solution is evaluated using several key metrics. Detection Accuracy measures the percentage of correctly classified packets, ensuring that legitimate requests are allowed while attack traffic is blocked effectively. False Positive Rate (FPR) quantifies the rate of legitimate requests wrongly classified as attacks, which is crucial in maintaining uninterrupted access for genuine users. False Negative Rate (FNR) determines the percentage of malicious requests that bypass detection, highlighting the system's ability to prevent attacks.

Another critical factor is Response Time, which assesses the time to analyze, filter, and redirect incoming packets. A lower response time indicates a more efficient system in mitigating DDoS threats. Additionally, System Load is monitored by evaluating CPU and memory consumption on honeypots under different attack intensities. This ensures that the system remains operational even under high-load conditions.

G. Assumptions & Limitations

The research assumes that the attack scenario accurately represents a real-world DDoS attack, allowing for realistic testing and evaluation. However, the honeynet is deployed in a single-network environment, meaning that modifications may be necessary for cloud-based or distributed deployments. The counterattack mechanism is developed strictly for educational and research purposes, ensuring ethical usage without any intent to cause harm. Finally, while the dataset used for training the ML model is extensive, it may not cover all evolving DDoS patterns. Future enhancements will be required to adapt to new attack techniques and maintain robust protection.

V. PROPOSED SOLUTION

The proposed solution involves deploying a honeynet-based defense mechanism to mitigate DDoS attacks using a combination of machine learning, traffic filtering, and load-balancing techniques. Incoming traffic is first intercepted by Honeypot 1, which classifies requests using an XGBoost-trained model based on the CICDDoS2019 dataset. Legitimate requests are forwarded to the target machine, while malicious traffic is blocked using iptables and logged for analysis. If traffic volume exceeds a predefined threshold, requests are redirected to Honeypot 2, which acts as a secondary filter and load balancer using HAProxy. Both honeypots run the ML model to ensure accurate classification. This layered approach ensures real-time attack detection, intelligent request filtering, and efficient load distribution, reducing the impact of DDoS attacks and maintaining optimal server performance.

VI. IMPLEMENTATION

A. Flow of the System

1) **Attack Initiation:** The attacker machine remotely controls two botnets via SSH and launches a LOIC-based DDoS attack on Honeypot 1.

2) **Traffic Filtering in Honeypot 1:** The XGBoost ML model classifies requests as legitimate or malicious. Malicious requests are blocked via iptables and logged, and Legitimate requests are forwarded to the target machine.

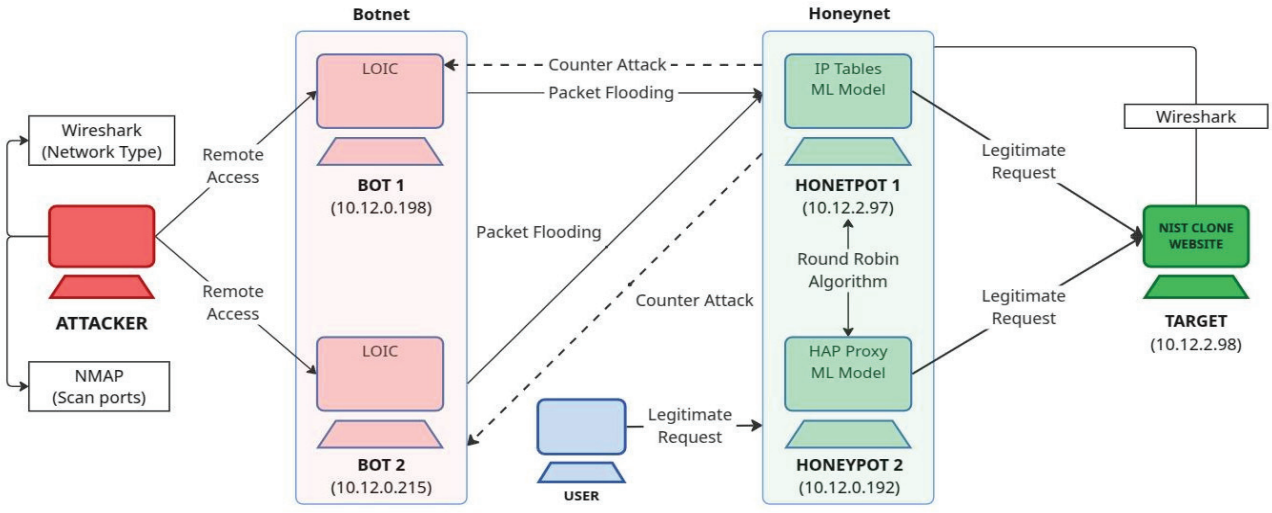

Fig. 1. System Architecture

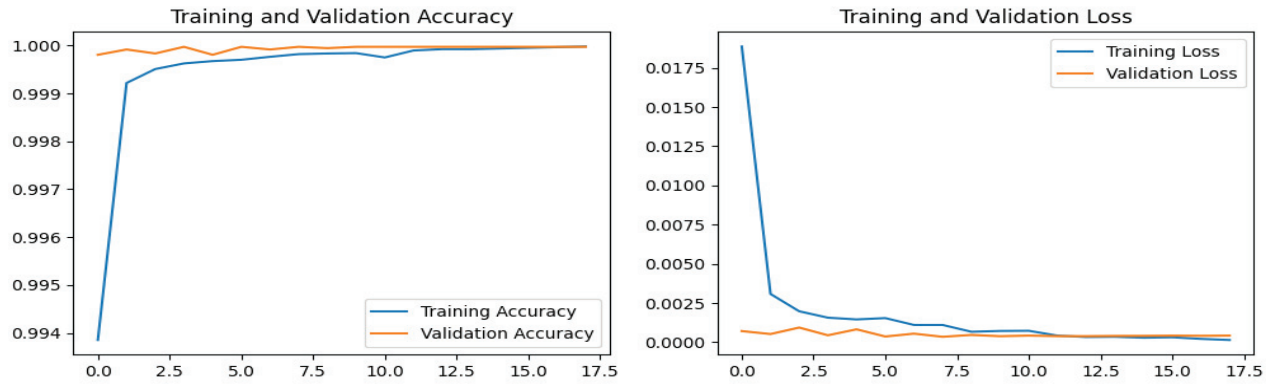

Fig. 2. ML model training & validation accuracy on the dataset

3) **Load Balancing in Honeypot 2:** If Honeypot 1 reaches a traffic threshold, HAProxy redirects traffic to Honeypot 2, where it applies the same ML-based filtering and forwards valid requests to the target machine.

4) **Target Machine Response:** The target machine receives only legitimate traffic, ensuring seamless access to the hosted website.

B. *Key Functionalities*

- Machine Learning-Based Filtering: The XGBoost model detects attack traffic in real time.
- Traffic Analysis & Logging: Wireshark captures incoming requests for attack detection and network analysis.
- Automated Blocking & Counterattack: iptables blocks attacking IPs while countermeasures mitigate threats.
- Load Balancing & Failover: HAProxy distributes traffic when Honeypot 1 reaches capacity.

C. *Development Stack*

1) Operating System: Ubuntu (All Machines)
2) Machine Learning Model: XGBoost (Trained on CICDDoS2019 Dataset)
3) Traffic Analysis: Wireshark
4) Firewall & Packet Filtering: iptables
5) Load Balancing: HAProxy
6) Attack Simulation: LOIC (Low Orbit Ion Cannon)

VII. SECURITY ANALYSIS

The honeynet-based DDoS mitigation system significantly enhances network resilience through real-time attack detection and response. By leveraging machine learning, the system efficiently identifies and blocks malicious traffic with minimal false positives and negatives. iptables and HAProxy integration ensure adaptive filtering and traffic distribution under heavy loads. However, the system assumes that attackers do not rapidly evolve attack patterns, and while effective for the current dataset, future updates may require adaptive model retraining to counter evolving threats.

VIII. RESULTS

The proposed honeynet-based DDoS mitigation system demonstrated high effectiveness in filtering malicious traffic and ensuring uninterrupted access to the target server. The machine learning-based classification achieved a detection accuracy of 99.99%, correctly identifying attack and legitimate traffic with minimal errors. The false positive rate (FPR) remained at 0.01%, ensuring that genuine users were not mistakenly blocked, while the false negative rate (FNR) was recorded at 0.02%, indicating a strong ability to detect and mitigate DDoS attacks. The response time for traffic filtering was under 0.5 milliseconds per request, allowing real-time decision-making without noticeable delays. Under high attack intensities, CPU utilization on Honeypot 1 peaked at 78%, triggering the load-balancing mechanism to distribute excess traffic to Honeypot 2, which resulted in a balanced CPU load of 45% across both honeypots. These results confirm that the proposed system efficiently filters out attack traffic, adapts to increased loads, and maintains network stability under DDoS conditions.

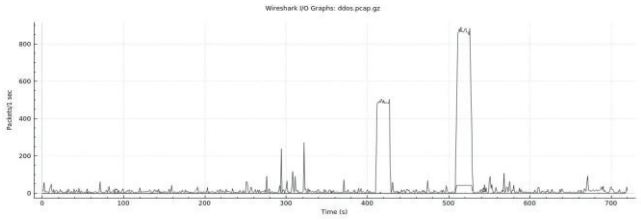

Fig. 3. Wireshark traffic analysis (in real time)

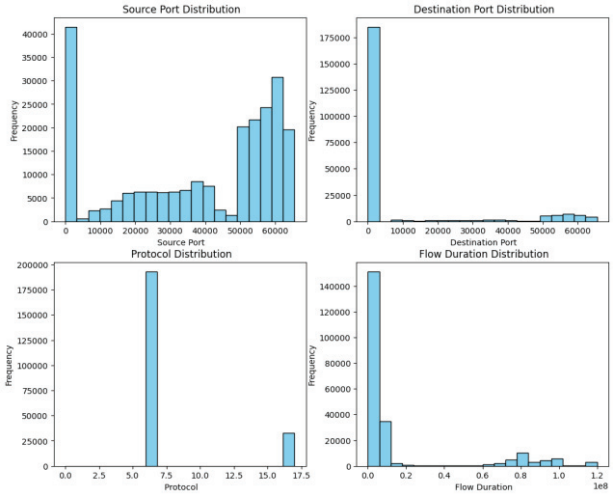

Fig. 4. DDoS dataset analysis

IX. CONCLUSION

This research presents an intelligent honeynet-based DDoS defense system integrating machine learning, firewall filtering, and load balancing to protect target servers from botnet-driven attacks. The experimental setup demonstrates effective traffic classification, attack mitigation, and system scalability. By leveraging an XGBoost-trained model, the system accurately detects malicious requests and ensures seamless service availability. Future work will focus on enhancing adaptability through continuous ML model updates and extending the system for cloud-based deployments.

REFERENCES

[1] A. K. M. Habib, A. Imtiaz, D. Tripura, Md. Faruk, A. Hossain, I. Ara, S. Sarker and A. F. M. Abadin, "Distributed denial-of-service attack detection short review: issues, challenges, and recommendations," in Bulletin of Electrical Engineering and Informatics, vol. 14, pp. 438-446, 2025, doi: 10.11591/eei.v14i1.8377.

[2] J. Xue, J. Ren, L. Feng and L. Wang, "An Analysis of Worm Dynamics with Honeypot Feedback in Scale-Free Networks," vol. 52, Issue 1, pp. 90-102, 2025.

[3] O. El Kouari, S. Lazaar and T. Achoughi, "Fortifying industrial cybersecurity: a novel industrial internet of things architecture enhanced by honeypot integration," in International Journal of Electrical and Computer Engineering (IJECE), vol.15, no.1, pp. 1089-1098, ISSN 2088-8708, 2025, doi: 10.11591/ijece.v15i1.pp1089-1098.

[4] D. M. A. A. Afraji, J. Lloret and L. Peñalver, "Deep learning-driven defense strategies for mitigating DDoS attacks in cloud computing environments," in Cyber Security and Applications, vol. 3, 100085, ISSN 2772-9184, 2025, doi: 10.1016/j.csa.2025.100085.

[5] T. Mahjabin, Y. Xiao, G. Sun and W. Jiang, "A survey of distributed denial-of-service attack, prevention, and mitigation techniques," in International Journal of Distributed Sensor Networks, 13(12), 2017, doi: 10.1177/1550147717741463.

[6] E. Gelenbe and M. Nasereddin, "Adaptive Attack Mitigation for IoV Flood Attacks," in IEEE Internet of Things Journal, vol. 12, no. 5, pp. 4701-4714, 2025, doi: 10.1109/JIOT.2025.3529615.

[7] B. Alhijawi, S. Almajali, H. Elgala, H. B. Salameh and M. Ayyash, "A survey on DoS/DDoS mitigation techniques in SDNs: Classification, comparison, solutions, testing tools and datasets," in Computers and Electrical Engineering, vol. 99, ISSN 0045-7906, 107706, 2022, doi: 10.1016/j.compeleceng.2022.107706.

[8] M. A. O. Rabah, H. Drid, Y. Medjadba and M. Rahouti, "Detection and Mitigation of Distributed Denial of Service Attacks Using Ensemble Learning and Honeypots in a Novel SDN-UAV Network Architecture," in IEEE Access, vol. 12, pp. 128929-128940, 2024, doi: 10.1109/ACCESS.2024.3443142.

[9] J. X. Huang, S. Zhou, N. Savage and W. Zhang, "A Distributed Cloud Honeypot Architecture," in IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC), pp. 1176-1181, 2021, doi: 10.1109/COMPSAC51774.2021.00162.

[10] M. Tayyab, B. Belaton and M. Anbar, "ICMPv6-Based DoS and DDoS Attacks Detection Using Machine Learning Techniques, Open Challenges, and Blockchain Applicability: A Review," in IEEE Access, vol. 8, pp. 170529-170547, 2020, doi: 10.1109/ACCESS.2020.3022963.

[11] S. Dong and M. Sarem, "DDoS Attack Detection Method Based on Improved KNN With the Degree of DDoS Attack in Software-Defined Networks," in IEEE Access, vol. 8, pp. 5039-5048, 2020, doi: 10.1109/ACCESS.2019.2963077.

[12] A. Hirsi et al., "Comprehensive Analysis of DDoS Anomaly Detection in Software-Defined Networks," in IEEE Access, vol. 13, pp. 23013-23071, 2025, doi: 10.1109/ACCESS.2025.3535943.

[13] D. Mohammed Sharif, H. Beitollahi and M. Fazeli, "Detection of Application-Layer DDoS Attacks Produced by Various Freely Accessible Toolkits Using Machine Learning," in IEEE Access, vol. 11, pp. 51810-51819, 2023, doi: 10.1109/ACCESS.2023.3280122.

[14] J. A. Pérez-Díaz, I. A. Valdovinos, K. -K. R. Choo and D. Zhu, "A Flexible SDN-Based Architecture for Identifying and Mitigating Low-Rate DDoS Attacks Using Machine Learning," in IEEE Access, vol. 8, pp. 155859-155872, 2020, doi: 10.1109/ACCESS.2020.3019330.

[15] U. Islam, A. Al-Atawi, H. S. Alwageed, M. Ahsan, F. A. Awwad and M. R. Abonazel, "Real-Time Detection Schemes for Memory DoS (M-DoS) Attacks on Cloud Computing Applications," in IEEE Access, vol. 11, pp. 74641-74656, 2023, doi: 10.1109/ACCESS.2023.3290910.

[16] A. Sahi, D. Lai, Y. Li and M. Diykh, "An Efficient DDoS TCP Flood Attack Detection and Prevention System in a Cloud Environment," in IEEE Access, vol. 5, pp. 6036-6048, 2017, doi: 10.1109/ACCESS.2017.2688460.

[17] H. Lin, S. Cao, J. Wu, Z. Cao and F. Wang, "Identifying Application-Layer DDoS Attacks Based on Request Rhythm Matrices," in IEEE Access, vol. 7, pp. 164480-164491, 2019, doi: 10.1109/ACCESS.2019.2950820.

[18] J. Luo, X. Yang, J. Wang, J. Xu, J. Sun and K. Long, "On a Mathematical Model for Low-Rate Shrew DDoS," in IEEE Transactions on Information Forensics and Security, vol. 9, no. 7, pp. 1069-1083, July 2014, doi: 10.1109/TIFS.2014.2321034.

[19] N. Anand, M. A. Saifulla, R. B. Ponnuru, G. R. Alavalapati, R. Patan and A. H. Gandomi, "Securing Software Defined Networks: A Comprehensive Analysis of Approaches, Applications, and Future Strategies against DoS Attacks," in IEEE Access, doi: 10.1109/ACCESS.2024.3520478.

[20] Z. Li, H. Jin, D. Zou and B. Yuan, "Exploring New Opportunities to Defeat Low-Rate DDoS Attack in Container-Based Cloud Environment," in IEEE Transactions on Parallel and Distributed Systems, vol. 31, no. 3, pp. 695-706, 1 March 2020, doi: 10.1109/TPDS.2019.2942591.

[21] V. D. M. Rios, P. R. M. Inácio, D. Magoni and M. M. Freire, "Detection and Mitigation of Low-Rate Denial-of-Service Attacks: A Survey," in IEEE Access, vol. 10, pp. 76648-76668, 2022, doi: 10.1109/ACCESS.2022.3191430.

[22] L. Abdelrazek, R. Fuladi, J. Kövér, L. Karaçay and U. Gülen, "Detecting IP DDoS Attacks Using 3GPP Radio Protocols," in IEEE Access, vol. 12, pp. 24776-24790, 2024, doi: 10.1109/ACCESS.2024.3365425.

[23] A. T. K. Al-Khayyat and O. Nuri Ucan, "A Multi-Branched Hybrid Perceptron Network for DDoS Attack Detection Using Dynamic Feature Adaptation and Multi-Instance Learning," in IEEE Access, vol. 12, pp. 192618-192638, 2024, doi: 10.1109/ACCESS.2024.3508028.

[24] W. Zhijun, X. Qing, W. Jingjie, Y. Meng and L. Liang, "Low-Rate DDoS Attack Detection Based on Factorization Machine in Software Defined Network," in IEEE Access, vol. 8, pp. 17404-17418, 2020, doi: 10.1109/ACCESS.2020.2967478.

[25] M. V. O. De Assis, A. H. Hamamoto, T. Abrão and M. L. Proença, "A Game Theoretical Based System Using Holt-Winters and Genetic Algorithm With Fuzzy Logic for DoS/DDoS Mitigation on SDN Networks," in IEEE Access, vol. 5, pp. 9485-9496, 2017, doi: 10.1109/ACCESS.2017.2702341.

[26] W. Zhijun, L. Wenjing, L. Liang and Y. Meng, "Low-Rate DoS Attacks, Detection, Defense, and Challenges: A Survey," in IEEE Access, vol. 8, pp. 43920-43943, 2020, doi: 10.1109/ACCESS.2020.2976609.

[27] T. V. Phan and M. Park, "Efficient Distributed Denial-of-Service Attack Defense in SDN-Based Cloud," in IEEE Access, vol. 7, pp. 18701-18714, 2019, doi: 10.1109/ACCESS.2019.2896783.

[28] M. M. Rahman, S. Roy and M. A. Yousuf, "DDoS Mitigation and Intrusion Prevention in Content Delivery Networks using Distributed Virtual Honeypots," 2019 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT), Dhaka, Bangladesh, 2019, pp. 1-6, doi: 10.1109/ICASERT.2019.8934572.

[29] I. Sembiring, "Implementation of honeypot to detect and prevent distributed denial of service attack," 2016 3rd International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE), Semarang, Indonesia, 2016, pp. 345-350, doi: 10.1109/ICITACEE.2016.7892469.

[30] M. Du and K. Wang, "An SDN-Enabled Pseudo-Honeypot Strategy for Distributed Denial of Service Attacks in Industrial Internet of Things," in IEEE Transactions on Industrial Informatics, vol. 16, no. 1, pp. 648-657, Jan. 2020, doi: 10.1109/TII.2019.2917912.

[31] V. A. Memos and K. E. Psannis, "AI-Powered Honeypots for Enhanced IoT Botnet Detection," 2020 3rd World Symposium on

Communication Engineering (WSCE), Thessaloniki, Greece, 2020, pp. 64-68, doi: 10.1109/WSCE51339.2020.9275581.

[32] K. Gaur, K. Gaur, T. Sachdeva, M. Diwakar, P. Singh and N. K. Pandey, "Effective Security Mechanisms against Distributed Denial of Services," 2023 6th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 2023, pp. 1-5, doi: 10.1109/ISCON57294.2023.10111999.

[33] K. Wang, M. Du, S. Maharjan and Y. Sun, "Strategic Honeypot Game Model for Distributed Denial of Service Attacks in the Smart Grid," in IEEE Transactions on Smart Grid, vol. 8, no. 5, pp. 2474-2482, Sept. 2017, doi: 10.1109/TSG.2017.2670144.

[34] R. Venkatesan, G. Ashwin Kumar and M. R. Nandhan, "A NOVEL APPROACH TO DETECT DDOS ATTACK THROUGH VIRTUAL HONEYPOT," 2018 IEEE International Conference on System, Computation, Automation and Networking (ICSCA), Pondicherry, India, 2018, pp. 1-6, doi: 10.1109/ICSCAN.2018.8541209.

[35] A. Kyriakou and N. Sklavos, "Container-Based Honeypot Deployment for the Analysis of Malicious Activity," 2018 Global Information Infrastructure and Networking Symposium (GIIS), Thessaloniki, Greece, 2018, pp. 1-4, doi: 10.1109/GIIS.2018.8635778.

[36] F. Mayorga, J. Vargas, E. Álvarez and H. D. Martinez, "Honeypot Network Configuration through Cyberattack Patterns," 2019 International Conference on Information Systems and Computer Science (INCISCOS), Quito, Ecuador, 2019, pp. 150-155, doi: 10.1109/INCISCOS49368.2019.00032.

[37] Z. Aradi and A. Bánáti, "The Role of Honeypots in Modern Cybersecurity Strategies," 2025 IEEE 23rd World Symposium on Applied Machine Intelligence and Informatics (SAMI), Stará Lesná, Slovakia, 2025, pp. 000189-000196, doi: 10.1109/SAMI63904.2025.10883300.

[38] K. E. Silaen, F. L. Gaol, S. H. Supangkat and B. Ranti, "Threat Modeling for Honeypot Deployment," 2024 IEEE 10th Information Technology International Seminar (ITIS), Surabaya, Indonesia, 2024, pp. 57-61, doi: 10.1109/ITIS64716.2024.10845226.

[39] B. Li, Y. Xiao, Y. Shi, Q. Kong, Y. Wu and H. Bao, "Anti-Honeypot Enabled Optimal Attack Strategy for Industrial Cyber-Physical Systems," in IEEE Open Journal of the Computer Society, vol. 1, pp. 250-261, 2020, doi: 10.1109/OJCS.2020.3030825.

[40] C. Sun et al., "Application of Artificial Intelligence Technology in Honeypot Technology," 2021 International Conference on Advanced Computing and Endogenous Security, Nanjing, China, 2022, pp. 01-09, doi: 10.1109/IEEECONF52377.2022.10013349.

[41] M. U. Rana, O. Ellahi, M. Alam, J. L. Webber, A. Mehbodniya and S. Khan, "Offensive Security: Cyber Threat Intelligence Enrichment With Counterintelligence and Counterattack," in IEEE Access, vol. 10, pp. 108760-108774, 2022, doi: 10.1109/ACCESS.2022.3213644.