RESEARCH PAPER

EDoS-Aegis: A Proactive Shielding Framework against EDoS and DDoS Attacks for Enhanced Cloud Security

Suneetha Bandeela[1], Suneetha Bulla[2]

[1]*Research Scholar, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Green Fields, Vaddeswaram, Guntur District, A.P., INDIA, 522 302.*
suneetha.charita@gmail.com
[2]*Associate professor , Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Green Fields, Vaddeswaram, Guntur District, A.P., INDIA, 522 302*
suneethabulla@gmail.com

ABSTRACT
In recent years, cloud environments have faced escalating threats from Denial of Service (DoS) attacks, particularly Distributed Denial of Service (DDoS) and Economic Denial of Sustainability (EDoS) attacks. EDoS attacks, in particular, exploit cloud scalability to inflate costs for cloud customers and providers, creating economic strain. While existing mitigation strategies address certain aspects of these attacks, they remain limited in ensuring comprehensive protection for cloud customers and providers. This paper proposes a novel, proactive framework called the EDoS-Aegis System (EDoS-Aegis), designed to enhance network resilience and mitigate the economic impact of these attacks on cloud systems. The EDoS-Aegis framework is implemented on the customer's side, creating a robust protective layer that guards both customer networks and cloud providers from DDoS and EDoS attacks. It achieves this by focusing on precise traffic source verification, reducing response times, and safeguarding cloud scalability. Through effective filtering techniques based on queuing models, the framework selectively blocks malicious traffic while facilitating faster response times for legitimate users. The framework explores four hypothetical scenarios. Each scenario simulates requests from various sources, highlighting the system's reactions to legitimate and malicious users. A conceptual evaluation then follows, assessing the framework's effectiveness and identifying potential areas for improvement. This analysis will inform adjustments aimed at fortifying the framework against attacks that threaten cloud-based networks, paving the way for a more resilient defense system..

Keywords: N\A
How to cite this article: Bandeela S, Bulla S. EDoS-Aegis: A Proactive Shielding Framework against EDoS and DDoS Attacks for Enhanced Cloud Security. .Int J Drug Deliv Technol. 2026;16 (3s): 1007-1015; DOI: 10.25258/ijddt.16.3s.121

Source of support:. None
Conflict of interest: None

INTRODUCTION

Cloud computing has become essential for modern businesses, offering scalable, flexible, and cost-effective solutions for data storage, processing, and networking [1]. However, with the increasing adoption of cloud services, security threats targeting these infrastructures have escalated, especially Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks [2]. These attacks overwhelm cloud resources, causing service interruptions and financial losses. While several mitigation techniques have been proposed, existing solutions struggle to provide adequate protection for the dynamic, scalable nature of cloud environments [3].

Among the newer threats facing cloud systems is the Economic Denial of Sustainability (EDoS) attack. EDoS attacks target the cloud's economic model by exploiting auto-scaling mechanisms, generating high volumes of seemingly legitimate traffic that cause unnecessary resource scaling and inflate costs for the customer [4]. This attack type is particularly problematic for small and medium-sized enterprises, as prolonged EDoS attacks can significantly increase operational costs, placing severe financial strain on affected businesses [5]. Current EDoS mitigation strategies, such as rate limiting, traffic pattern analysis, and anomaly-based detection, offer partial solutions. However, these approaches are typically reactive, addressing malicious traffic only after it impacts the system. Such methods often struggle to keep pace with sophisticated EDoS attacks, which evolve to bypass existing detection systems, exacerbating financial and operational challenges [6]. This gap highlights the need for proactive and comprehensive solutions tailored to the unique demands of cloud scalability.

To address these limitations, this paper proposes a novel framework, the EDoS-Aegis System, designed to protect cloud customers from EDoS and DDoS attacks. The EDoS-Aegis framework operates on the customer's side, creating a robust protective layer that emphasizes source verification and precise traffic filtering. This approach prevents cost escalation by blocking malicious traffic before it forces unnecessary scaling, thus reducing both economic and resource strain for cloud providers and customers alike [7] [8] [9].

**Author for Correspondence: Suneetha Bandeela*

Central to the EDoS-Aegis framework is the use of queuing models to filter incoming traffic selectively. By applying filtering techniques based on traffic source verification, the framework can differentiate between legitimate and malicious requests, minimizing the risk of false positives and improving overall system efficiency. This proactive filtering not only reduces response times for legitimate users but also maintains scalability in cloud environments without sacrificing performance. To evaluate the EDoS-Aegis framework's efficacy, four hypothetical traffic scenarios are presented, simulating different request patterns and sources. These scenarios highlight the framework's capabilities in distinguishing between genuine and malicious traffic, demonstrating its potential to mitigate the economic impact of EDoS attacks on cloud systems. This evaluation establishes a foundation for future research and enhancement of the EDoS-Aegis framework, aiming to provide cloud environments with a more resilient and cost-effective defense against evolving EDoS threats.

This paper is organized as follows. Section 2 presents a comprehensive literature survey, reviewing existing approaches to mitigating Denial of Service (DoS), Distributed Denial of Service (DDoS), and Economic Denial of Sustainability (EDoS) attacks in cloud environments. It highlights the limitations of current solutions and the need for a proactive framework specifically designed to tackle the unique challenges posed by EDoS attacks. Section 3 details the architecture of the proposed model, outlining its components and the underlying design principles of the EDoS-Aegis System. Section 4 delves into the EDoS-Aegis Framework's Scenarios, describing four hypothetical cases used to evaluate the model's ability to differentiate between legitimate and malicious traffic. Section 5 presents the results of these simulations, demonstrating the framework's effectiveness in mitigating the economic impact of EDoS attacks, reducing response times, and safeguarding cloud scalability. Finally, Section 6 offers conclusions drawn from the study, summarizing the contributions of the EDoS-Aegis framework.

2. Literature Survey

This survey incorporates recent research on mitigating Denial of Service (DoS), Distributed Denial of Service (DDoS), and Economic Denial of Sustainability (EDoS) attacks in cloud environments, focusing on existing strategies and their limitations

The increasing adoption of cloud computing has attracted attention from cyber attackers, leading to a rise in security threats such as Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. These attacks aim to exhaust cloud resources, causing service disruptions and financial losses [10]. Traditional approaches to mitigating DoS and DDoS attacks focus on filtering mechanisms, rate limiting, and anomaly detection[11]. While these methods are effective to an extent, they often fall short in the context of cloud environments, where scalability and performance are crucial. For instance, anomaly-based detection systems may incorrectly classify legitimate traffic as malicious, leading to increased false positives and impacting user experience[12].

A relatively newer threat, Economic Denial of Sustainability (EDoS) attacks, specifically targets the economic model of cloud infrastructure by exploiting its auto-scaling feature. EDoS attacks involve generating a high volume of seemingly legitimate traffic to trigger unnecessary scaling, thereby inflating costs for the customer. Unlike traditional DDoS attacks that aim to crash servers temporarily, EDoS attacks exploit cloud service scalability to create sustained financial strain [13]. Mitigating EDoS attacks is challenging because traditional traffic filtering and anomaly detection approaches may not distinguish between legitimate and malicious traffic effectively, especially when attacks mimic typical user behavior [14]. This has led researchers to explore specialized mitigation techniques tailored to EDoS threats.

Several approaches to EDoS mitigation have been proposed, with rate limiting and pattern-based filtering among the common techniques. However, these techniques have limitations. Rate limiting, for instance, may restrict the scalability benefits of cloud infrastructure by limiting traffic indiscriminately, affecting legitimate users during peak times [15].

Similarly, pattern-based filtering techniques are often unable to detect sophisticated EDoS attacks, which may vary traffic patterns to evade detection. Machine learning-based detection methods, such as those employing deep learning and neural networks, have shown promise by analyzing traffic behavior to identify abnormal patterns [16]. However, these methods are typically reactive, addressing malicious traffic only after it has impacted the system.

This research has increasingly focused on developing proactive filtering approaches to enhance the mitigation of Economic Denial of Sustainability (EDoS) attacks in cloud computing environments. One notable method proposed in [17] involves the integration of machine learning algorithms to design adaptive filters that can identify and respond to EDoS attacks in real time. These adaptive filters continuously analyze incoming traffic patterns, learning from historical data to improve detection accuracy. By dynamically updating their filtering rules, they can adapt to evolving attack strategies, thereby reducing the likelihood of missed detections. This real-time adaptability is a significant advantage over static filtering techniques, which may fail to address new or sophisticated threats. However, the implementation of such machine learning–driven systems requires substantial computational resources to process and classify traffic data continuously. The computational demand can, in turn, increase the operational and infrastructure costs for cloud service providers. Additionally, the complexity of deploying and maintaining such adaptive models can present technical challenges, especially for smaller organizations. Despite these drawbacks, the approach remains promising for large-scale cloud providers where detection accuracy is a top priority.

Another promising solution is source verification to confirm the legitimacy of incoming requests before they impact the system. This technique has been shown to be effective in mitigating EDoS attacks by focusing on request origin, although it faces challenges in deployment across distributed cloud environments [19]. Nonetheless, these studies highlight the potential of using proactive, customer-side filtering techniques, which act before malicious traffic triggers auto-scaling. Such techniques are beneficial in reducing response times for legitimate users while safeguarding cloud infrastructure from financial exploitation by EDoS attacks.

3. Architecture of the proposed EDoS-Aegis

The workflow of the figure 1 begins with incoming traffic from both legitimate users and attackers. When a request is received, it first encounters the Verifier Node, which checks the request against white list and black list entries. If a user's IP is on the white list, they are likely a known, trusted entity, and their request may bypass additional verification steps for quicker processing. If the IP is on the black list, the request is blocked immediately, preventing further interaction with the system. For requests not matched on either list, the Verifier Node performs further checks. Suspicious requests may then be subject to OTT (On-the-Threshold Testing), which assesses whether a user is legitimate or potentially malicious.

If a request still cannot be verified as legitimate, it is sent to the Client Puzzle Server. Here, the server issues a computational puzzle or challenge to the user. Legitimate users can solve these puzzles quickly, allowing them to proceed, while bots or attackers face significant delays or resource exhaustion, discouraging further attack attempts.

Once requests pass through these verification stages, they reach the DNS Server. The DNS server ensures that verified traffic is routed correctly, sending it toward A Set of Green Nodes. These green nodes act as additional verification points or load balancers, helping distribute and manage incoming requests while filtering out any remaining suspicious traffic. The green nodes analyze traffic patterns and may block requests that exhibit malicious behavior, adding another layer of protection. Traffic that successfully passes through the green nodes reaches the Filtering Router, which acts as the final checkpoint before the Protected Server.

The filtering router applies a last layer of filtering to ensure that only clean, verified traffic reaches the protected server. By the time requests reach this point, the system has thoroughly filtered out malicious traffic, allowing only legitimate users access to the protected server, which provides the desired cloud services. This multi-layered approach ensures effective protection against Economic Denial of Sustainability (EDoS) and Distributed Denial of Service (DDoS) attacks, minimizing disruption for genuine users while guarding against costly, malicious traffic. Here's an explanation of each module in the provided EDoS Aegis system diagram:

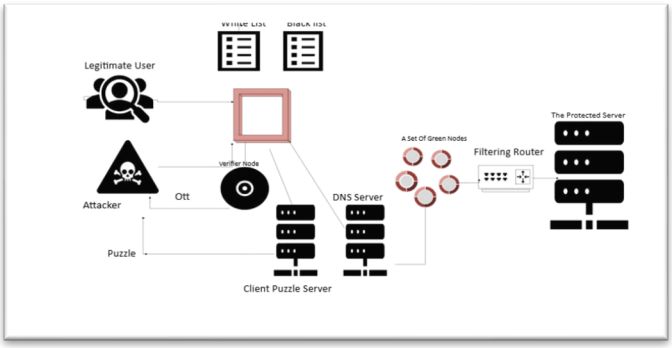

Figure 1: EDoS-Aegis Architecture1

Legitimate User: This represents a genuine user who is trying to access the cloud services. The system aims to ensure that requests from legitimate users are prioritized and processed without delay. The traffic from legitimate users is directed through the system to verify their authenticity before reaching the protected server.

Attacker: The attacker symbolizes malicious entities attempting to execute an Economic Denial of Sustainability (EDoS) attack or a Distributed Denial of Service (DDoS) attack. These attackers send a large volume of requests that mimic legitimate traffic to trigger cloud auto-scaling mechanisms and increase costs for the cloud service provider or customer.

White List / Black List: These lists serve as basic filtering mechanisms.

White List: This contains known, verified IP addresses or entities that are recognized as legitimate and can bypass certain levels of verification. This helps reduce latency for trusted users.

Black List: This contains IP addresses or entities known to be malicious or associated with previous attack patterns. Any requests from these sources are blocked or redirected to prevent them from accessing the protected server.

Verifier Node: The verifier node is responsible for authenticating incoming requests. It performs initial checks on each request to determine if the source is a legitimate user or a potential attacker. The verifier node may apply various verification techniques, such as analyzing request patterns, checking against white/black lists, and assessing request origin.

OTT (On-the-Threshold Testing): This module applies additional tests to determine the legitimacy of suspicious requests that couldn't be classified as safe or malicious by the verifier node. The OTT may involve computational challenges or puzzles to assess if the requestor is a real user or a bot.

Client Puzzle Server: The client puzzle server is an anti-DDoS and EDoS module that issues computational puzzles

to users whose legitimacy is unclear. If a request is suspected to be malicious, the client puzzle server requires the client to solve a computational puzzle before gaining access. Legitimate users can solve these puzzles with minimal delay, while it creates a resource drain on bots or attackers attempting to flood the system with requests.

DNS Server: The DNS server in this framework directs legitimate traffic to the appropriate paths. When requests are verified, the DNS server can route them to the protected server, minimizing delays for verified users. Additionally, it may work with other modules to prevent attackers from finding or overloading the protected server.

A Set of Green Nodes: Green nodes act as additional verification or load-balancing points within the system. They could serve as decoys or filters to further distinguish legitimate requests from malicious ones. These nodes help distribute incoming requests and further analyze patterns to offload some verification from the main filtering router.

Filtering Router: This module is a crucial part of the system's defense, sitting at the gateway of the protected server. It receives traffic from green nodes and applies the final layer of filtering to block any malicious traffic that may have bypassed previous layers. The filtering router is configured to only pass legitimate requests through to the protected server, enhancing security.

The Protected Server: This is the main server hosting the actual cloud service or application that needs protection. The entire EDoS-Aegis system aims to protect this server from malicious traffic, allowing only verified legitimate requests. The protected server can then serve genuine users without experiencing the negative impact of EDoS or DDoS attacks.

4. EDoS-Aegis Framework's Scenarios

The proposed EDoS-Aegis framework deals with incoming packets by categorizing them into four distinct scenarios to determine the legitimacy of users and protect the system from malicious attacks. It utilizes temporary and permanent white and black lists to streamline the packet handling process.

1) Scenario of Testing the First Packet

1. When a user sends a packet to the protected server, the firewall intercepts it and checks if the source IP address is on the whitelist or blacklist.
2. If the source IP is not found on any list, the packet is forwarded to the verifier node for further evaluation.
3. The verifier node sends a Graphical Turing Test (GTT) to the user to verify their legitimacy.
4. If the user passes the GTT, the verifier sends a positive acknowledgment to the firewall, and the source IP is added to the Temporary Whitelist (TWL).If the user fails, a negative acknowledgment is sent, the request is denied, and the source IP is added to the Temporary Blacklist (TBL) with a timestamp.
5. For users who pass the GTT, the firewall forwards the packet to the DNS server, which routes it through green nodes and the filtering router to reach the protected server.
6. The requested data is sent back to the user, completing the initial interaction process.

2) Scenario of Testing a Random Second Packet (Legitimate User)

1. Upon receiving a second packet, the firewall checks the source IP address against its lists, including the Temporary Whitelist (TWL).
2. If the source IP is in the TWL, the firewall either allows the packet to pass as legitimate or forwards it to the Client Puzzle Server for further verification if selected for additional testing.
3. The client puzzle server sends a crypto puzzle to the user to confirm legitimacy.
4. If the user solves the puzzle, a positive acknowledgment is sent to the firewall; otherwise, a negative acknowledgment is sent.
5. If the puzzle is not solved, the request is denied, and the source IP is removed from the TWL. If the puzzle is solved, the source IP is moved from the Temporary Whitelist (TWL) to the Permanent Whitelist (PWL).
6. The firewall forwards the packet to the DNS server, which routes it through green nodes and the filtering router to the protected server. The requested data is then delivered back to the user..

3) Scenario of Testing a Second Packet (Malicious User)

1. If the source IP is in the Temporary Blacklist (TBL), the firewall compares the timestamps of the current and previous packets to detect repeated malicious activity.
2. If the timestamps indicate repeated malicious intent, the request is denied, and the source IP is moved to the Permanent Blacklist (PBL).
3. If the timestamps differ, the firewall forwards the packet to the Verifier Node for another Graphical Turing Test (GTT). A positive acknowledgment allows the process to continue; a negative acknowledgment results in denial and transfer to the PBL.
4. For users passing the GTT, the packet is sent to the Client Puzzle Server for a crypto puzzle test.
5. If the puzzle is solved, the packet is forwarded to the protected server, and the user's details are removed from the TBL. If the puzzle is failed, the request is denied, and the source IP is moved to the PBL.
6. Based on these steps, malicious users are either blocked permanently or temporarily, ensuring no legitimate requests from malicious users pass through.

4) Scenario of Checking Subsequent Packets from Permanent Lists (PWL and PBL)

1. The firewall checks whether the source address of the incoming packet is in the Permanent Whitelist (PWL) or the Permanent Blacklist (PBL).
2. If the source address is in the PWL, the firewall forwards the packet directly to the protected server via the DNS server, green nodes, and filtering router, granting the user seamless access.
3. If the source is incorrectly listed in the PWL, the firewall removes the source address from the PWL to maintain list accuracy.
4. If the source address is in the PBL, the request is denied immediately, preventing the packet from reaching the server.
5. For blocked requests from PBL entries, the firewall updates the timestamp in the PBL to record the latest blocked attempt for monitoring purposes.

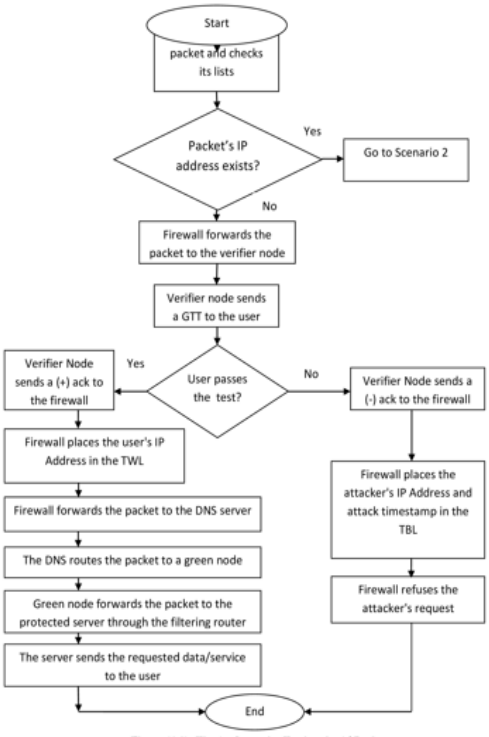

Figure 2: The first Scenario: Testing the first packet

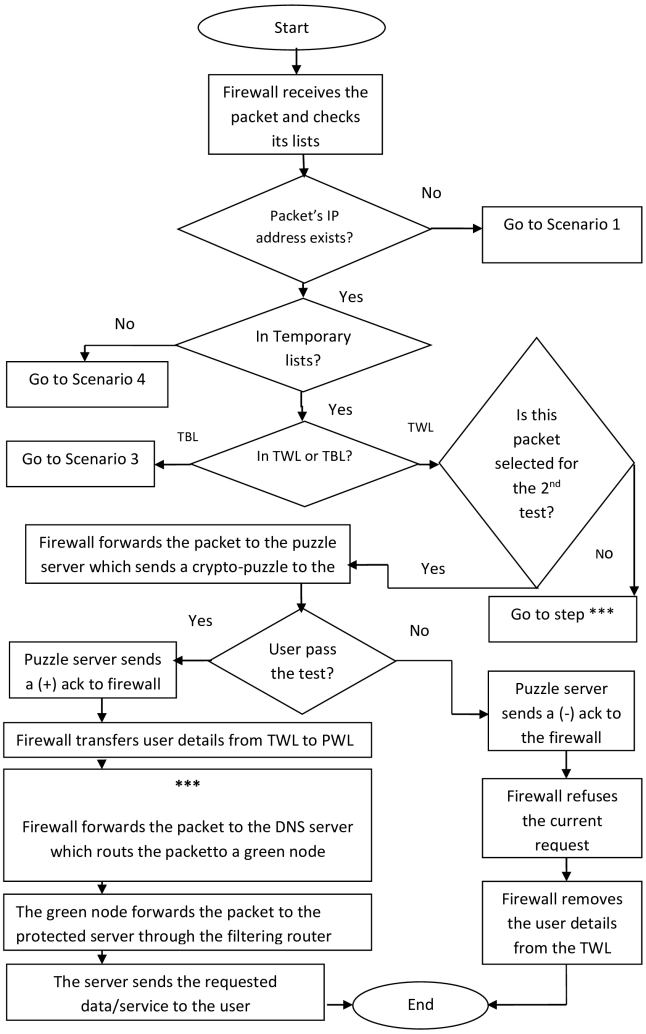

Figure 3: The 2nd Scenario:Testing the 2nd packet of the User in the TWL

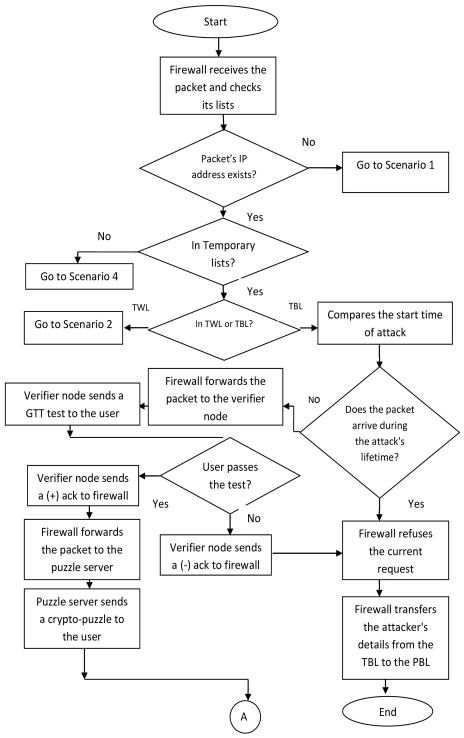

Figure 4: The 3rd Scenario:Testing the 2nd packet of the User in the TWL

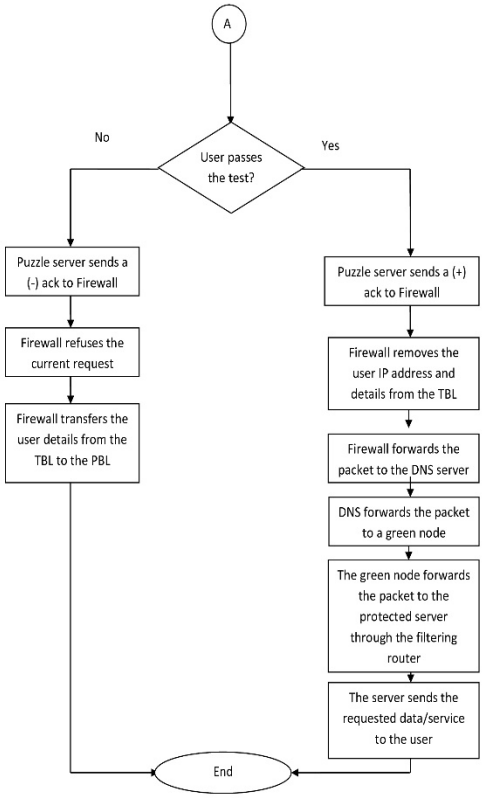

Figure 5: The 3rd Scenario Continued:Testing the 2nd packet of the User in the TBL

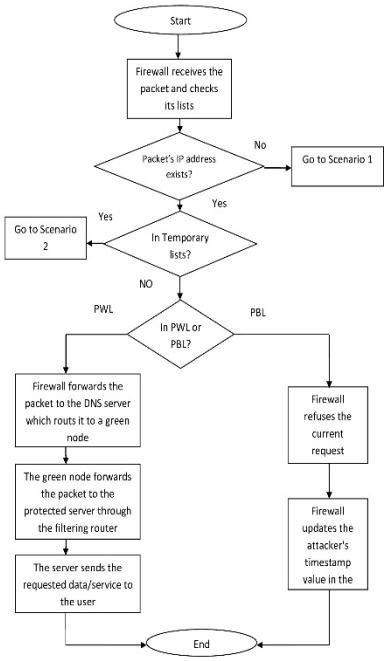

Figure 6: The 4th Scenario:Checking the Subsequent Packets of the Users in the Permanent List [Blackand White]

EDoS- Aegis framework introduces some thoughtful improvements over previous solutions, particularly in its nuanced handling of verification and response time. Here's a breakdown of the key benefits and how they differentiate your framework:

- Balanced Verification Process: Many prior solutions either perform extensive, repeated checks for all incoming packets (leading to high response times) or verify only one packet (which can be insufficient for effectively filtering out attacks). DDoS-MS addresses this by examining only two packets, achieving both verification robustness and lower response latency. This approach minimizes the impact on legitimate users while maintaining high network security.

- Selective IP List Management: The framework's approach to managing whitelists and blacklists is unique in that it avoids rigidly moving IP addresses between lists based on single tests. By removing an IP from the whitelist if a user fails the secondary puzzle test (and vice versa for blacklist entries), the framework maintains a flexible, resilient stance. This strategy prevents users from being overly penalized for isolated failures, which is valuable in situations with fluctuating network conditions or user behaviors.

- Cloud Scalability Protection: By ensuring that the verification mechanism does not interfere with the cloud's ability to scale, the framework maintains a balance between security and resource flexibility. This design consideration is crucial for services that need to handle variable traffic loads without compromising on availability.

- Enhanced Response Time: The DDoS-MS framework's selective packet examination ensures that legitimate users are not delayed unnecessarily, which is an improvement over systems like the DaaS framework that may impact user experience due to high response times.

- Two-Phase Testing (GTT and Puzzle): The combined use of the Gateway Throttling Test (GTT) and a puzzle mechanism adds an extra layer of security, where passing or failing the GTT alone doesn't dictate the final decision. This layered test approach allows the framework to retain legitimate users while ensuring attackers face more barriers.

DDoS- Aegis is innovative in minimizing the verification load and maintaining a balanced, flexible whitelist/blacklist management approach, which enhances resilience without compromising scalability or response times. These strategic improvements could make DDoS-MS a valuable addition to cloud-based security solutions focused on DDoS and EDoS mitigation.

5. Results

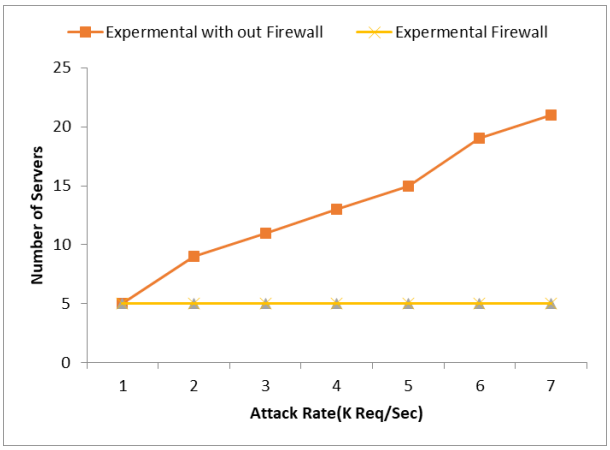

Figure 7: Total number of running servers in the cloud datacenter

Figure 7 compares the effect of an "Experimental Firewall" versus no firewall on the number of servers required to handle increasing attack rates, measured in thousands of requests per second (K Req/Sec.

The number of servers required increases sharply as the attack rate grows. This indicates that, without a firewall, the system has to allocate more resources (servers) to handle the high volume of incoming requests, likely due to an inability to filter out malicious traffic effectively. EDOS-Aegis remains flat across all attack rates, indicating that the number of servers remains constant (at about 5 servers) regardless of the attack rate. This suggests that the firewall is effectively mitigating the impact of the attack, reducing the need for additional resources.

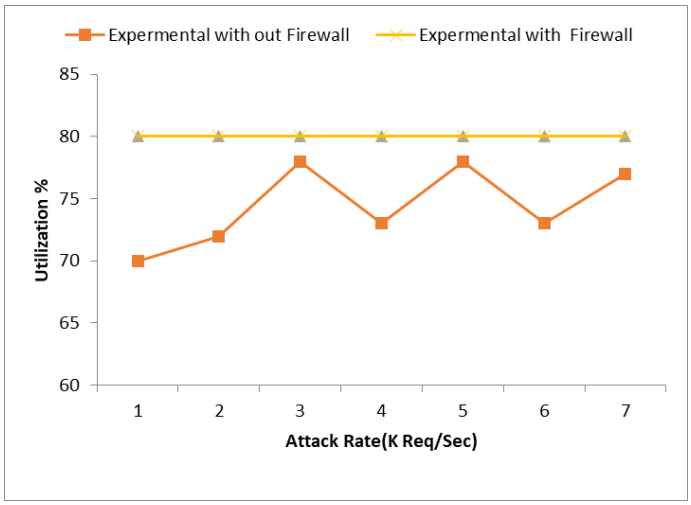

Figure 8: Utilization of Cloud in the EDOS and DDOS

Figure 8 illustrates the utilization percentage of the system with and without the "EDOS-Aegis" as the attack rate increases.The utilization percentage fluctuates as the attack rate increases. It generally stays between 70% and 80%, with peaks and drops as the attack rate rises. This fluctuation suggests that, without a firewall, the system experiences inconsistent load handling, likely due to unfiltered attack traffic that intermittently strains the resources. The utilization percentage of with EDOS-Aegis is steady, staying at around 80% regardless of the attack rate. This consistency indicates that the firewall effectively manages incoming requests, preventing attack traffic from impacting the system's utilization level significantly.

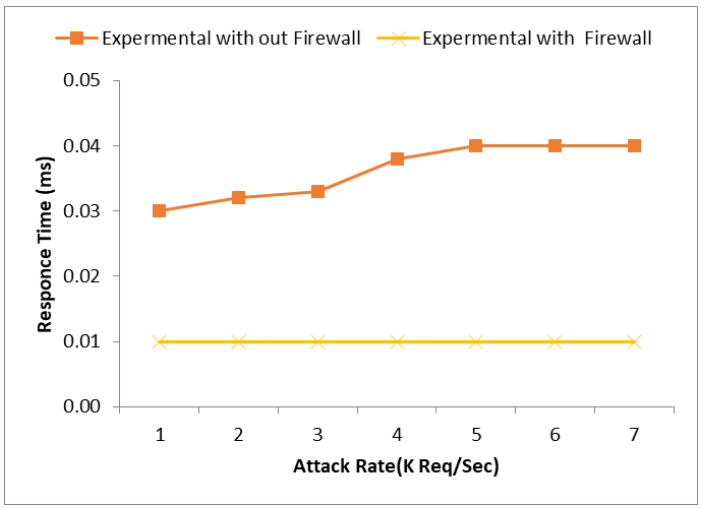

Figure 9: Response Time of Cloud in the EDOS and DDOS

Figure 9 illustrates the impact of system elasticity on response time under varying attack rates, comparing performance **with** and **without** a firewall. In the non-firewall configuration, response times increase gradually from about 0.031 ms at 1 K requests/sec to approximately 0.040 ms beyond 5 K requests/sec, indicating that the system struggles to sustain low latency as the workload intensifies. By contrast, the firewall-enabled setup demonstrates strong elasticity, maintaining a stable response time of around 0.01 ms across all tested attack rates. This stability reflects the system's ability to dynamically allocate and manage resources to absorb sudden traffic surges without degrading performance. As highlighted in *Ali et al.* (2023), such elasticity is crucial for minimizing processing bottlenecks and maintaining service quality during workload fluctuations. The results confirm that integrating adaptive filtering mechanisms, such as a firewall, not only mitigates EDoS-related performance drops but also reinforces the system's capacity to respond rapidly to changing demand levels, thereby enhancing both responsiveness and operational efficiency.

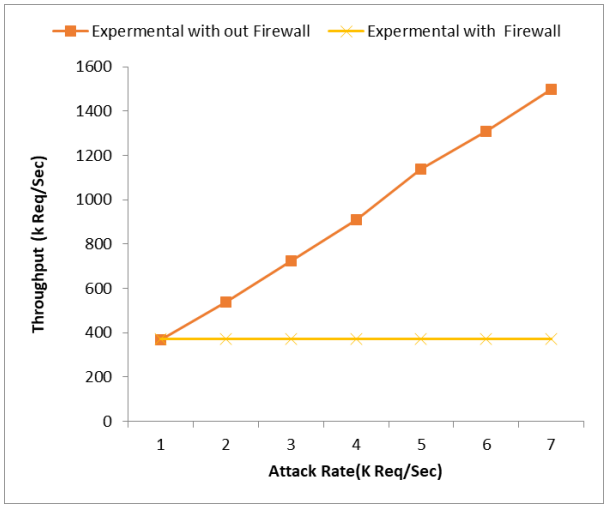

Figure 10: Throughput of Cloud in the EDOS and DDOS

Figure 10 reveals a notable disparity in throughput between the system operating with a firewall and the one without it. In the absence of a firewall, throughput declines more sharply as the attack rate increases, indicating that malicious traffic consumes a significant portion of system resources. Conversely, the firewall-enabled configuration sustains higher and more consistent throughput, demonstrating its ability to filter illegitimate requests before they impact service capacity. This performance stability highlights the firewall's role in preserving system efficiency under adverse network conditions.

6. Conclusion and Discussions

The EDoS-Aegis framework is a proactive and innovative solution to counter DDoS and EDoS attacks. It uses a Graphical Turing Test for initial verification and a crypto puzzle for secondary verification to identify bots. The dual-layered firewall system, with temporary and permanent white/blacklists, ensures legitimate users face minimal latency while blocking malicious sources effectively. Deployed at the customer edge, it protects both clients and providers, leveraging techniques like user classification, server location hiding, and randomization. This multi-layered approach enhances security and guarantees service availability even during attacks**.** For future work, the framework can be enhanced by integrating advanced AI-driven methods to improve the accuracy and adaptability of the Graphical Turing Test, particularly in distinguishing between human users and sophisticated bots. One promising direction is using reinforcement learning to dynamically adjust puzzle difficulty based on observed attack patterns, enabling the system to respond in real time to evolving threats. This adaptive mechanism could balance security strength with user convenience, ensuring that legitimate users are not burdened by excessive verification complexity. Additionally, incorporating accessibility features will ensure the framework remains usable across diverse user demographics, including individuals with disabilities, further broadening its effectiveness and inclusivity..

REFERENCE

1. Hashem, I. A. T., et al. (2020). "The rise of 'big data' on cloud computing: Review and open research issues." Information Systems.
2. Panchal, S., et al. (2021). "DDoS attack detection and mitigation in cloud computing." Journal of Cloud Computing: Advances, Systems and Applications.
3. Ahmad, M., et al. (2021). "A Survey of Distributed Denial of Service (DDoS) Attack Detection Mechanisms in Cloud Computing." IEEE Access.
4. Abhishek, S., et al. (2019). "Mitigating Economic Denial of Sustainability Attacks in Cloud Computing Using Source Verification." International Journal of Advanced Computer Science and Applications.
5. Ali, M., et al. (2023). "Economic Denial of Sustainability (EDoS) in Cloud Computing and Mitigation Strategies." Journal of Cloud Computing.
6. Dinh, T. T., et al. (2022). "Detection of EDoS Attack in Cloud Environment Using Machine Learning Techniques." Security and Privacy in Communication Networks.
7. Mumtaz, S., et al. (2023). "Proactive Detection and Mitigation of EDoS Attacks Using Machine Learning-Based Source Filtering." IEEE Transactions on Cloud Computing.
8. Iqbal, R., et al. (2021). "A Queuing Model-Based Approach for Traffic Filtering to Combat DDoS and EDoS Attacks." Computers & Security.
9. Raj, A., et al. (2023). "A Framework for Economic Denial of Sustainability Attack Mitigation in Cloud

Computing Environments." Future Generation Computer Systems.
10. Hashem, I. A. T., et al. (2020). "The rise of 'big data' on cloud computing: Review and open research issues." Information Systems.
11. Panchal, S., et al. (2021). "DDoS attack detection and mitigation in cloud computing." Journal of Cloud Computing: Advances, Systems and Applications.
12. Ahmad, M., et al. (2021). "A Survey of Distributed Denial of Service (DDoS) Attack Detection Mechanisms in Cloud Computing." IEEE Access.
13. Abhishek, S., et al. (2019). "Mitigating Economic Denial of Sustainability Attacks in Cloud Computing Using Source Verification." International Journal of Advanced Computer Science and Applications.
14. Ali, M., et al. (2023). "Economic Denial of Sustainability (EDoS) in Cloud Computing and Mitigation Strategies." Journal of Cloud Computing.
15. Dinh, T. T., et al. (2022). "Detection of EDoS Attack in Cloud Environment Using Machine Learning Techniques." Security and Privacy in Communication Networks.
16. Kokila, R., et al. (2021). "DDoS Detection and Analysis in Cloud Computing Using Machine Learning Techniques." International Journal of Computer Applications.
17. Iqbal, R., et al. (2021). "A Queuing Model-Based Approach for Traffic Filtering to Combat DDoS and EDoS Attacks." Computers & Security.
18. Raj, A., et al. (2023). "A Framework for Economic Denial of Sustainability Attack Mitigation in Cloud Computing Environments." Future Generation Computer Systems.
19. He, X., et al. (2023). "Intelligent DDoS Detection for Cloud Security Using Neural Networks." IEEE Transactions on Cloud Computing..