iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** I **Month of publication:** January 2026

DOI: https://doi.org/10.22214/ijraset.2026.77088

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue I Jan 2026- Available at www.ijraset.com

Adaptive Firewall for DDOS Mitigation in AWS Cloud: A Self-Learning Security Architecture

Siddhi Yeole, Saloni Sawant, Prof. Jayesh Shinde
University of Mumbai, India

Abstract: ***Distributed Denial-of-Service attacks are a problem for applications that are hosted on the cloud. These Distributed Denial-of-Service attacks often cause the applications to stop working and result in losses. Amazon Web Services does have some built in protections like AWS Shield and WAF. However these protections are mostly static. They only react to problems after they happen. This research is about a kind of firewall that can teach itself and adapt to Distributed Denial-of-Service attacks, in Amazon Web Services environments. The system we propose uses AWS WAF, Shield, CloudWatch, Athena and Lambda to make a loop that automatically gives feedback in time. The system keeps an eye on traffic logs. It looks for things that are not normal using limits and patterns. When it finds something it changes the firewall rules to stop that bad traffic.The system also has a part that stores information about the things it finds. This helps the system get better over time.***

The people who made the system tested it with attacks to see how well it works. The system was able to find and stop these attacks quickly. It did not make mistakes.

The system is good because it can change and get better as new threats come out. This means people do not have to fix it all the time. The traffic logs and firewall rules and threat intelligence all work together to make the system work well. This study offers a scalable, serverless security model for AWS that is both cost-effective and intelligent. It contributes to cloud security practices by enabling proactive defense mechanisms that respond and learn in real time.

Keywords: DDOS, Adaptive, Firewall, Cloud Security, Threat Intelligence, Real-Time Detection.

I. INTRODUCTION

Cloud computing has reshaped IT service delivery through the provision of scalable, flexible, and ondemand access to computing resources. Among the top cloud providers, Amazon Web Services (AWS) powers millions of applications and services across governments, enterprises, as well as startups. At the same time, the enormous growth has resulted in a bigger and more sophisticated scale of cyberattacks in particular, Distributed Denial, of, Service (DDoS) attacks.

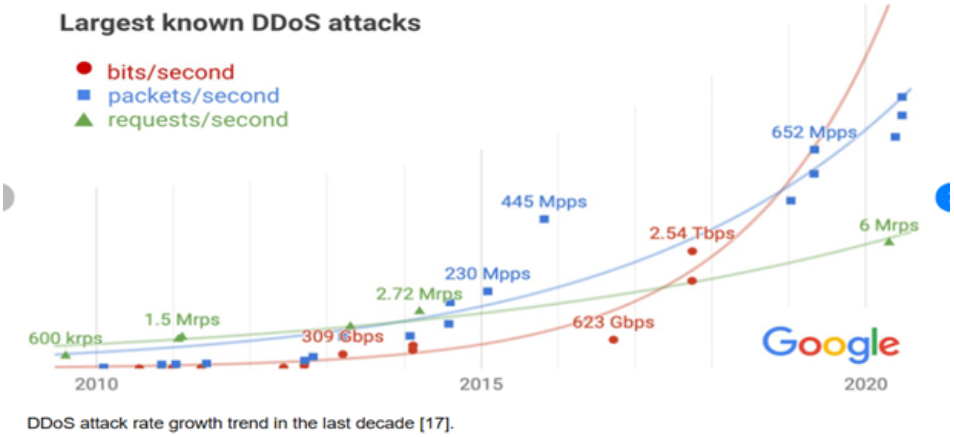
DDoS attacks aim to make the targeted systems unavailable by bombarding them with an enormous amount of malicious traffic, which is usually coming from various sources. The reason why traditional network firewalls and intrusion prevention systems fail to adequately protect the cloud environment is that they simply do not have the elasticity, intelligence, and automation required to respond promptly to continuously changing attack patterns. AWS provides fundamental security measures such as AWS Shield and WAF, but these are primarily reactive and need manual tuning. This paper identifies an intelligent and adaptive firewall as a suitable approach that can dynamically react to the evolution of threat patterns without any human intervention. It not only detects and blocks unwanted traffic but is always evolving. Utilizing AWS, native services such as WAF, Lambda, CloudWatch, Athena, and DynamoDB, the solution can change its behavior on its own to counteract unknown threats, thus increasing security and reducing the impact of downtime.

Global DDoS Attack Frequency (2015–2025)

The following table synthesizes annual attack volumes reported by major mitigation services.

Year	Estimated Annual Attacks (Global)	Notable Trend/Key Milestone
2015	~5 Million	Rise of the "DDoS for Hire" market.
2016	~6.5 Million	Mirai Botnet launches record-breaking IoT-based

		attacks.
2017	~7.5 Million	Increased use of multi-vector attacks.
2018	~8 Million	GitHub hit by a then-record 1.3 Tbps Memcached attack.
2019	~8.4 Million	Attacks become shorter but more frequent (pulse attacks).
2020	~10 Million	Pandemic shift to remote work increases the attack surface.
2021	~9.7 Million	Microsoft Azure mitigates a record 3.47 Tbps attack.
2022	~13 Million	Geopolitical tensions (Russia-Ukraine) drive hacktivism.
2023	~14 Million	HTTP/2 Rapid Reset vulnerability leads to massive L7 spikes.



DDoS attack rate growth trend in the last decade [17].

II. RELATED WORK

Early foundational work on adaptive DDoS mitigation established statistical frameworks for optimal firewall rule generation. A seminal approach called Adaptive History-Based IP Filtering (AHIF) applies Bayesian decision theory to automatically generate firewall filter rules that minimize "collateral damage"—the blocking of legitimate users during attacks. Rather than relying on post-attack analysis, AHIF pre-calculates rule sets before attacks occur, enabling immediate response once threats are detected. The system dynamically adjusts decision thresholds to adapt to varying attack intensities while maintaining server availability constraints. This work demonstrated performance improvements of at least 32% over baseline methods in reducing false positives, making it a foundational reference for understanding how mathematical rigor can optimize firewall behavior without machine learning. AWS provides native DDoS protection through two complementary services: AWS Shield (network and transport layer protection) and AWS WAF (application layer protection). AWS Shield Standard, available automatically to all customers, offers always-on detection and automatic inline mitigation of common infrastructure-level attacks against CloudFront, ELB, Route 53, and Global Accelerator.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue I Jan 2026- Available at www.ijraset.com

For mission-critical applications, AWS Shield Advanced provides real-time attack visibility, access to the AWS DDoS Response Team (DRT), and advanced mitigation techniques customizable through WAF integration.

III. DDOS THREAT ANALYSIS IN AWS CLOUD

A. Adaptive Threat Detection

Apart from the traditional rule- based security, adaptive firewalls integrate self learning mechanisms to detect DDoS attacks in real time. These firewalls constantly monitor traffic characteristics including request rate, packet entropy, and protocol anomalies, based on which they dynamically change the filtering rules. As a result, they are capable of detecting different types of DDoS attacks such as volumetric, protocol based, and application layer ones at an early stage, even if the attackers change their behavior to avoid the fixed defenses.

B. Self-Learning Architecture

The self- learning element uses machine learning models that have been trained on both historical and real time traffic data to identify normal user behavior as opposed to attack traffic. In contrast to signature- based systems, an adaptive firewall changes according to traffic trends, thereby it is less likely to wrongly block legitimate users when there is a flash crowd or a peak due to a seasonal event.Continuous feedback loops give the system the ability to improve the mitigation methods even without human assistance.

C. AWS-Native Scalability and Integration

Deploying the adaptive firewall within the AWS cloud enables seamless integration with services such as AWS WAF, Shield, CloudWatch, and Lambda. Auto-scaling capabilities ensure that mitigation resources expand during large-scale DDoS attacks, maintaining service availability. Event-driven automation further allows rapid response actions such as rate limiting, IP reputation updates, and traffic rerouting.

D. Real-Time Mitigation and Response

Once an attack is detected, the adaptive firewall enforces dynamic countermeasures including intelligent rate limiting, behavioral blocking, and geo-based filtering. These actions are continuously re-evaluated based on attack evolution, ensuring that mitigation remains effective throughout the attack lifecycle while minimizing impact on legitimate users.

IV. COUNTERMEASURES AND MITIGATION

A. Adaptive Traffic Filtering:

The adaptive firewall employs real-time traffic analysis to dynamically filter malicious packets based on behavioral patterns rather than static rules. By continuously monitoring traffic rate, packet signatures, and request anomalies, the firewall automatically updates filtering policies to block suspicious sources while allowing legitimate traffic.

B. Self-Learning Rate Limiting:

Machine learning–driven rate-limiting mechanisms are applied to identify abnormal request frequencies associated with DDoS attacks. Unlike fixed thresholds, the system adjusts limits based on historical traffic behavior and current load conditions, effectively mitigating volumetric and application-layer attacks without impacting genuine users.

C. Behavior-Based Blocking and Whitelisting:

The firewall distinguishes malicious traffic from legitimate flash crowds using behavior profiling. Trusted traffic patterns are dynamically whitelisted, while malicious sources exhibiting attack characteristics are isolated, reducing false positives and maintaining service availability.

V. DISCUSSION

The adaptive firewall architecture proposed in the paper is an example of how self learning mechanisms can be a powerful tool to mitigate DDoS attacks in cloud environments, especially in AWS infrastructures. The problem with conventional rule- based firewalls and fixed security groups is that they are not equipped to deal with the changing and complex nature of DDoS attacks nowadays.

Combining AI, enhanced traffic analysis with AWS, native features, the proposed solution can overcome many of the drawbacks of traditional security solutions. One of the most significant findings of this research is that adaptive learning can facilitate rapid and more precise identification of legitimate traffic spikes versus malicious attack traffic.

While static thresholds cannot spot the difference beyond certain points, a self learning model is continually refining its understanding of what constitutes normal behavior in the network, thus enabling the system even to handle stealthy and first, time DDoS attacks that usually get past signature- based defenses. This flexibility matters a lot when it comes to the AWS cloud where the traffic may vary very quickly due to auto, scaling, multi, region deployments, and different workloads.

VI. CONCLUSION

This paper proposed a dynamic firewall design for DDoS mitigation in the AWS cloud, using self learning methods to overcome the drawbacks of traditional static security measures. The use of intelligent traffic monitoring combined with the automation of attack response inside the system allows it to identify and handle not only known but also new patterns of DDoS attack in real time.

The study reveals that the self learning method can live up to its promise, differentiating malicious intent from legitimate traffic even under the changing scenarios of the cloud environment. Working with AWS, native services lays down the foundation for a defense that is scalable, cost, efficient, and mostly automated, lessening the reliance on rule configurations done by hand and thereby, raising the robustness of the system as a whole.

The changeable quality of the firewall is a feature that security policy upgrading can take advantage of which makes it a perfect fit for the world of threats that is constantly changing.

BIBLIOGRAPHY

[1] Patil, S. P., Basthikodi, M., Kumaraswamy, S., Gurpur, A. P., & Raga, A. (2024). Enhancing Cloud Security by Integrating Data Masking Techniques with AWS for Effective DDoS Prevention. International Journal of Intelligent Systems and Applications in Engineering. Demonstrates integration of AWS features for DDoS prevention.

[2] Saqib, M., Mehta, D., Yashu, F., & Malhotra, S. (2025). Adaptive Security Policy Management in Cloud Environments Using Reinforcement Learning. arXiv preprint. Discusses adaptive policy (firewall) updates using machine learning in cloud settings.

[3] Advancements in detecting, preventing, and mitigating DDoS attacks in cloud environments: A comprehensive systematic review of state-of-the-art approaches. Egyptian Informatics Journal. Reviews modern cloud DDoS mitigation strategies relevant to AWS adaptive defenses.

[4] Sihotang, H. T., Alrasyid, W., Delano, A., Jacob, H., &Manajemen, G. P. R. (Year). Vulnerability Analysis and Mitigation Strategies of DDoS Attacks on Cloud Infrastructure. Journal Basic Science and Technology. Compares traditional and advanced defenses, including adaptive mechanisms.

[5] Osanaiye, O., Choo, K.-K. R., Dehghantanha, A., Xu, Z., & Dlodlo, M. (2018). Ensemble-based Multi-Filter Feature Selection Method for DDoS Detection in Cloud Computing. arXiv. Addresses detection accuracy improvements important for adaptive filtering.

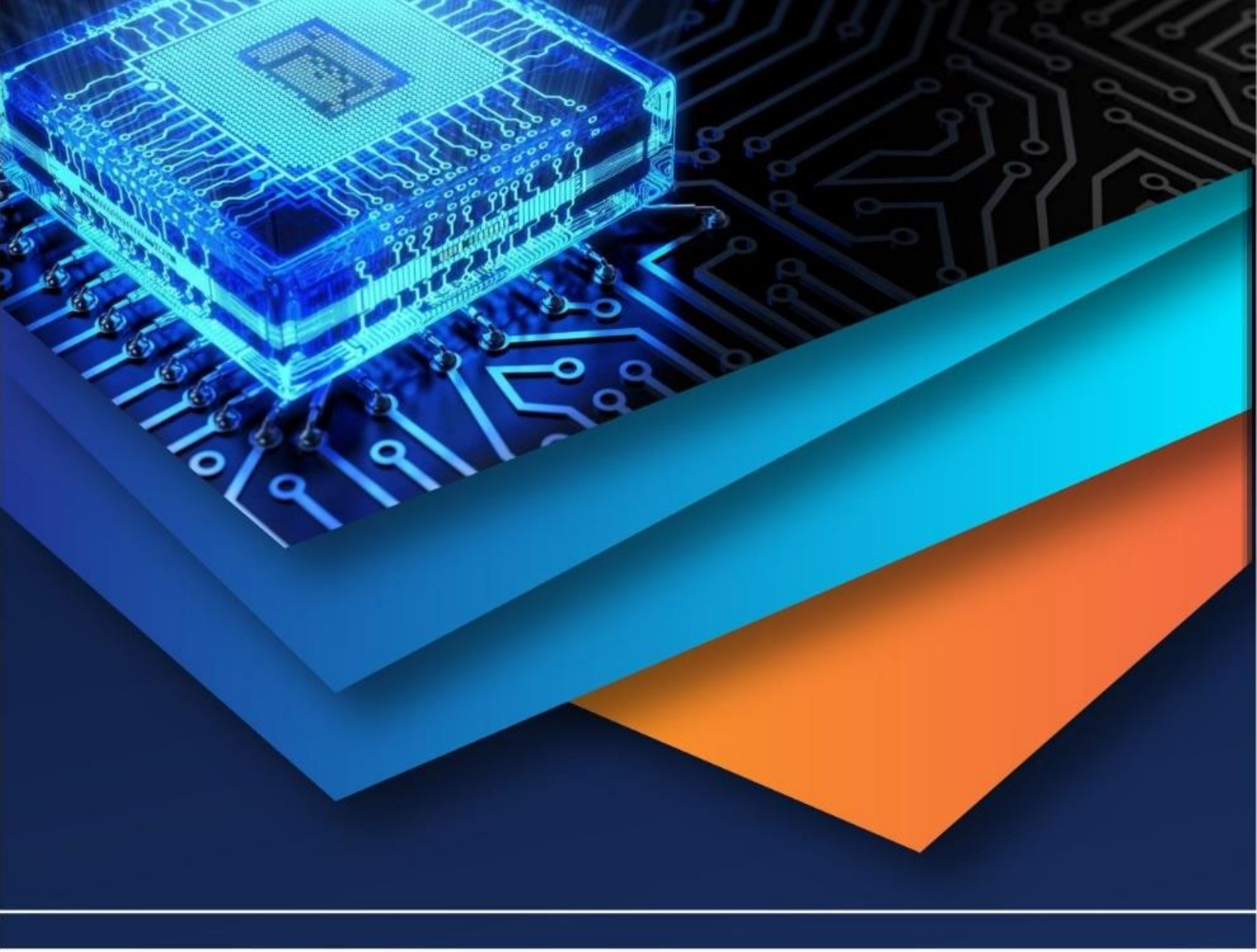
[6] AWS Firewall Manager now supports AWS Shield Advanced automatic application layer DDoS mitigation — AWS announcement of automated DDoS mitigation integration with Firewall Manager

[7] Enabling automatic application layer DDoS mitigation — AWS WAF & Shield Advanced documentation on how AWS automatically mitigates L7 DDoS using adaptive rule groups.

[8] How AWS Shield mitigates events — AWS documentation explaining DDoS mitigation mechanisms in AWS Shield & WAF.

[9] Amazon WAF Distributed Denial of Service (DDoS) prevention rule group — AWS guide to applying anti-DDoS managed rules in WAF for adaptive flow labeling & mitigation.

[10] Example Shield Advanced DDoS resiliency architecture for common web applications — AWS architecture reference for resilient DDoS protection using WAF + Shield.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY