Al-imad Journal of Humanities and Applied Sciences (AJHAS)
مجلة العماد للعلوم الإنسانية والتطبيقية
ISSN: 3106-0323
Volume 2 – Issue 2 – 2026
Pages 673-679

Intelligent Resource Allocation for Modern Cyber Defense

Mohamed Hmadi [1.2], Mouemer Elhjmelad Elriheemi [3]
[1,3] Department of Computer Science, Faculty of Science, Azzaytuna University, Tarhuna, Libya
[2] Department of Cyber Security, University of Darence Ahlahlia, Libya
[1.2]m.hmadi@azu.edu.ly, [3]m.alhjmelad@azu.edu.ly

التخصيص الذكي لموارد للدفاع السيبراني الحديث

محمد حمادي [1، 2] ، معمر الحاج ميلاد الرحيمي [3]
[1]، [3] قسم علوم الحاسوب، كلية العلوم، جامعة الزيتونة، ترهونة، ليبيا
[2] قسم الأمن السيبراني، جامعة دارنس الأهلية، ليبيا

Received: 15-07-2026; Accepted: 18-08-2026; Published: 28-08-2026

Abstract:
This paper conclusively demonstrates a strong correlation between the number of packets captured and the available bandwidth, supporting the theory that network performance to direct impacts of the attacks. From the data gathered, the most significant attack types were network scanning, packet retransmission, and leakage of information. Furthermore, security measures were proposed including, but not limited to, removal of outdated firewall configurations, increased scrutiny on processes, and the tightening of monitored traffic filters. There was also a proposal made on the ability to assess risk priority and trigger intrusion detection systems automatically. These findings prove that relying solely on behavioral analysis is insufficient; adding real-time supervision significantly improves the cybersecurity posture and uninterrupted service availability of multifaceted networks.

Key Words: Distributed denial of service (DDoS) attack, network traffic databases, firewall rules, cybersecurity.

الملخص
اثبتت هذه الورقة البحثية ان هناك علاقة قوية بين عدد الحزم الملتقطة وعرض النطاق الترددي المتاح، مما يدعم نظرية أن أداء الشبكة يتأثر بشكل مباشر بالهجمات .ومن خلال البيانات التي جمعت، تبين أن أبرز أنواع الهجمات هي مسح الشبكة، وإعادة إرسال الحزم، وتسريب المعلومات. وقدمنا اقتراحات تدابير أمنية تشمل على سبيل المثال لا الحصر، إزالة إعدادات جدار الحماية القديمة، وزيادة التدقيق في العمليات، وتشديد فلاتر حركة المرور المراقبة. كما اقترحنا إمكانية تقييم أولوية المخاطر وتفعيل أنظمة كشف التسلل تلقائيا. تثبت هذه النتائج أن الاعتماد على التحليل السلوكي وحده غير كاف؛ إذ إن إضافة الإشراف في الوقت الفعلي يُحسن بشكل كبير من وضع الأمن السيبراني واستمرارية توافر الخدمة للشبكات المتعددة.

الكلمات المفتاحية: هجوم جحب الخدمة الموزع (*DDoS*)، قواعد بيانات حركة مرور الشبكة، قواعد جدار الحماية، الأمن السيبراني.

1. Introduction and Motivation

Cyber threats and network security are of paramount importance in light of technological expansion and increasing reliance on electronic services. This research responds to the challenges arising from abnormal network traffic and excessive resource utilization in information systems, which calls for in-depth analysis to detect suspicious patterns and provide practical recommendations for enhancing cybersecurity. While these defense approaches yield respectable outcomes, plenty is yet to be explored in order to meet the open challenges faced by these domains. The research analyzes network traffic logs and system usage data to identify vital indicators that may indicate potential cyberattacks or resource management issues. The research relies on comprehensive data including packet rates, bandwidth, and memory and processor utilization to paint a clear picture of the risks and provide effective solutions.

1.2. Main contribution

This research problem challenges a sudden rise in abnormal network traffic indicators accompanied by abnormal system resource consumption. Possibly such abnormal behavior may give rise to external attacks such as a distributed denial of service (DDoS) attack or an internal nefarious activity. This behavior coincides with high memory and processor utilization rates; therefore, possibly unauthorized activities are occupying resources. The data presents a more complex relationship between traffic and resource utilization, where the number of packets is strongly correlated with bandwidth. In contrast, memory and processor consumption levels are very weakly correlated, further complicating the differentiation between legitimate and suspicious activity. This data whittles down the accurateness of analysis mechanisms based on performance indicators and network traffic. This hence demands the need to develop smart tools and detection systems based on high-level algorithms to defend cybersecurity.

Thus, an integrated of network metrics supports early detection of attacks and continuity of critical operations.

2. CYBERATTACK TRAFFIC

A distributed denial of service (DDoS) attack is a type of cyber-attack that aims to disrupt the service of a website, network, or server over the Internet by overwhelming it with a huge amount of requests or data, causing the service to stop or slow down significantly, and becoming unavailable to users.

2.1. DDOS PROTECTION SERVICES

Use DDoS protection services, such as Cloud flare, AWS Shield, and Azure DDoS Protection, Load Balancing: Distributes requests across multiple servers. Rate Limiting: Specifies the number of requests allowed from a single user, monitor system and Artificial Intelligence: For early detection of suspicious patterns. These are specialized platforms designed to detect and mitigate large-scale DDoS attacks by filtering malicious traffic before it reaches your infrastructure. Global Anycast Network: Spreads traffic across multiple data centers. Rate Limiting & WAF (Web Application Firewall): Helps block abnormal traffic patterns. Always-on protection for common attack types.

2.2 AWS SHIELD, TWO TIERS:

a) Standard: Free, automatic protection for all AWS customers.

b) Advanced: Paid service with enhanced protections, DDoS response team (DRT), and integration with AWS WAF.

2.3 Azure DDoS Protection, Two tiers:

a) Basic: Integrated into the platform.

b) Standard: Offers deeper telemetry, custom mitigation policies, and better protection for public IP resources.

3. Load Balancing

Load balancers distribute incoming traffic across multiple backend servers. This, Prevent overloading any-single server and Improve application availability and reliability.

Work in tandem with auto-scaling groups to handle sudden traffic spikes both legitimate and malicious.(AWS Elastic Load Balancer (ELB),Azure Load Balancer and NGINX / HAProxy).

4. Rate Limiting

This technique restricts the number of requests a user or IP address can make within a certain timeframe. Helps prevent abuse from bots or API overuse.

Can be applied at different levels: per user, per API key, per IP, etc. Often integrated with DDoS services or implemented via WAF rules.

5. Traffic Analysis and Artificial Intelligence (AI)

Modern DDoS protection systems increasingly use AI and machine learning to detect anomalies early and respond automatically. Monitors baseline behavior and flags deviations. Detects sophisticated low-and-slow or application-layer attacks. Reduces false positives and improves accuracy over time

5.1 CENTRAL IDEA OF TRAFFIC ANALYSIS AND ARTIFICIAL INTELLIGENCE (AI)

In recent years, virtually all DDoS and network protection services have integrated AI and Machine Learning into their infrastructure for more precise and proactive anomaly detection and mitigation. They continuously track baseline metrics and detect deviations. Frustrates advanced low-and-slow or application-layer attacks. Uses historical data to refine processes and enhance precision over time. Including features, Behavioral analysis, Real-time threat intelligence and Adaptive rule sets based on historical data.

5.2 Practice Checklist

Strategy	Description
Use a DDoS Protection Service	Cloudflare, AWS Shield, Azure DDoS
Implement Load Balancing	Distribute traffic across servers
Apply Rate Limiting	Control request frequency
Enable Traffic Monitoring	Watch for unusual patterns
Integrate AI/ML Detection	Advanced threat detection
Regularly Update Security Policies	Adapt to new threats

5.3 COMBINED CLOUDFLARE, AWS SHIELD, AZURE DDOS

Feature	Cloudflare	AWS Shield	Azure DDoS
Layer 3/4 Protection	Yes	Yes	Yes
Layer 7 Protection	Yes (WAF)	Yes (WAF)	Yes (WAF)
Global Network	Yes (Anycast)	Regional (unless used with CloudFront)	Mostly regional
Rate Limiting	Yes	Yes (with WAF)	Yes
AI-Based Detection	Yes	Yes	Yes
Cost	Free tier available	Free (Standard), Paid (Advanced)	Free (Basic), Paid (Standard)

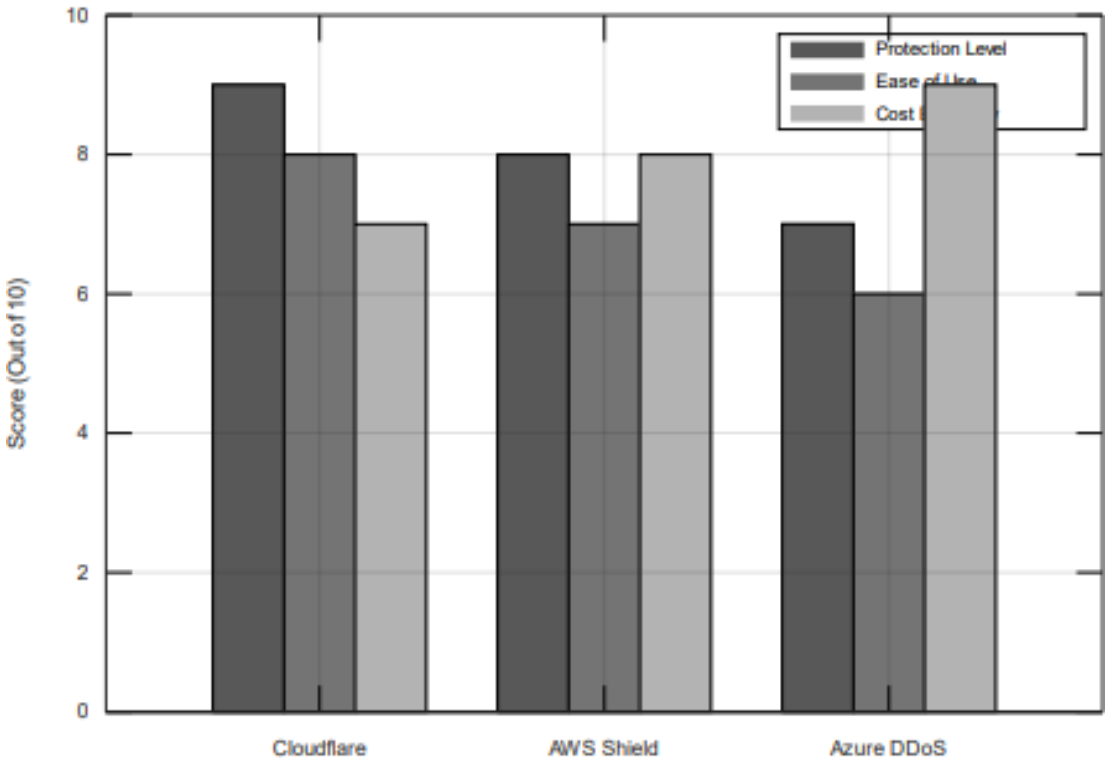

Figure (1): Octave Compare Cloudflare, AWS Shield, Azure DDoS Protection (Score out of 10)

5.4 *Generated Compare Cloudflare, AWS Shield, Azure DDoS Protection*

```
% Service names
services = {'Cloudflare', 'AWS Shield', 'Azure DDoS'};
% Example scores (out of 10)
protection_score = [9, 8, 7];  % Protection level
```



```
ease_of_use            = [8, 7, 6];   % Ease of integration
cost_efficiency = [7, 8, 9];          % Cost efficiency
% Plotting figure;
bar_width = 0.25;
x = 1:length(services);
b1 = bar(x, protection_score, bar_width); hold on;
b2 = bar(x + bar_width, ease_of_use, bar_width);
b3 = bar(x + 2*bar_width, cost_efficiency, bar_width);
% Customize
set(gca, 'XTick', x + bar_width, 'XTickLabel', services); legend('Protection Level', 'Ease of Use', 'Cost Efficiency'); title('Comparison of DDoS Protection Services'); ylabel('Score (Out of 10)');
grid on; hold off;
% Save image print('ddos_service_comparison.png', '-dpng');
disp('DDoS service comparison chart saved as dds_service_comparison.png');
```

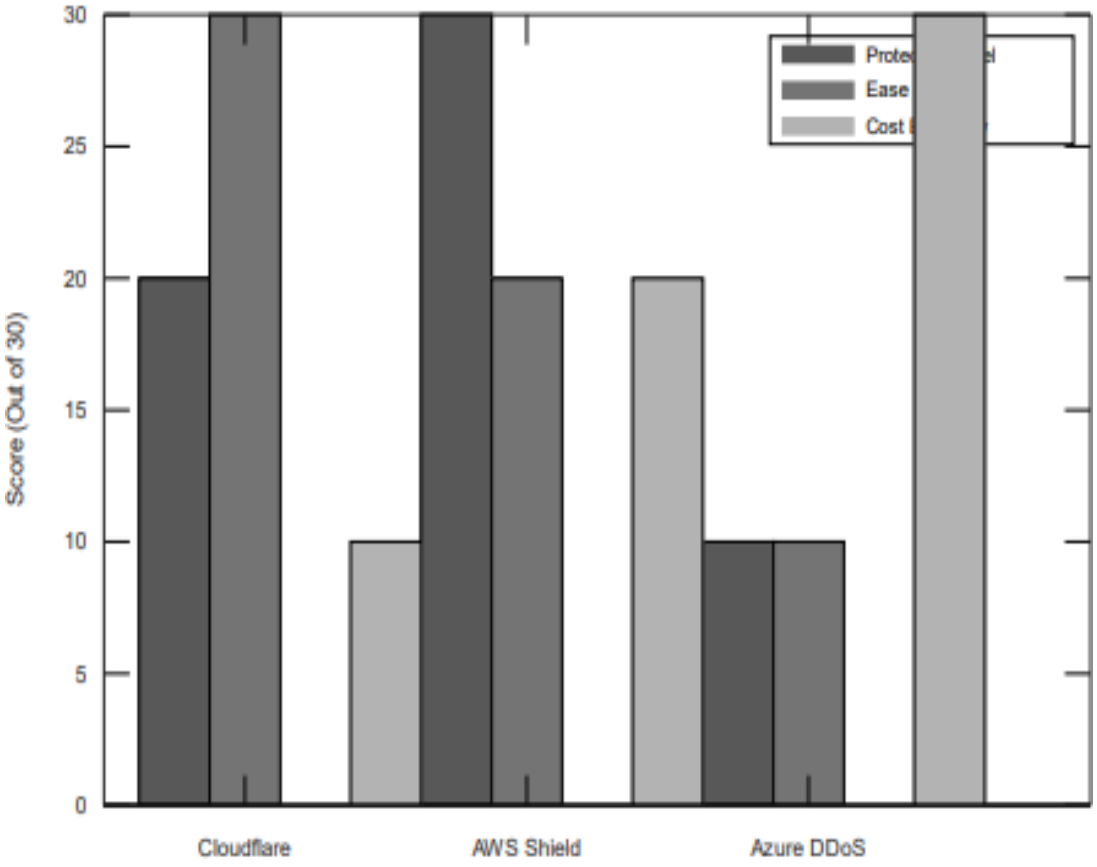

Figure (2): Octave Compare Cloudflare, AWS Shield, Azure DDoS Protection (Score out of 30).

5.5 *Generated Compare Cloudflare, AWS Shield, Azure DDoS Protection*

```
% Service names
services = {'Cloudflare', 'AWS Shield', 'Azure DDoS'};
% Example scores (out of 30)
protection_score = [20, 30, 10];  % Protection level
ease_of_use            = [30, 20, 10];  % Ease of integration
cost_efficiency = [10, 20, 30];         % Cost efficiency
% Plotting figure;
bar_width = 0.25;
x = 0.75:length(services);
b1 = bar(x, protection_score, bar_width); hold on;
b2 = bar(x + bar_width, ease_of_use, bar_width);
b3 = bar(x + 3*bar_width, cost_efficiency, bar_width);
% Customize
set(gca, 'XTick', x + bar_width, 'XTickLabel', services); legend('Protection Level', 'Ease of Use', 'Cost Efficiency'); title('Comparison of DDoS Protection Services'); ylabel('Score (Out of 30)');
grid on; hold off;
% Save image print('ddos_service_comparison.png', '-dpng');
disp('DDoS service comparison chart saved as dds_service_comparison.png');
```

6. CONCLUSION

A layered approach combining DDoS protection services, load balancing, rate limiting, and AI-driven traffic analysis provides strong defense-in-depth against DDoS attacks. Each layer plays a specific role, and together they offer resilience even during large-scale cyberattacks.

7. FUTURE WORK

DDoS protection will need to shift into intelligent and decentralized technologies that are more adaptive, especially as services become more digitally accessible. The approach is bound to change from mere filtering to a multilayered context security system that integrates identity verification as well as access control and network orchestration. Such a change is critical as the infrastructure becomes more digitized and systems become more complex.

References

[1]Kai Xu,Zemin Li,Nan Liang,Fanchun Kong,Shaobo Lei ,Shengjie Wang ,Agyemang Paul and Zhefu Wu “Research on Multi-Layer Defense against DDoS Attacks in Intelligent Distribution Networks”, Electronics , 10 September 2024.

[2]Kazeem B. Adedeji,Adnan M. Abu-Mahfouz and Anish M. Kurien , “DDoS Attack and Detection Methods in Internet-Enabled Networks: Concept, Research Perspectives, and Challenges, Journal of Sensor and Actuator Networks “, 6 July 2023

[3]Anshuman Singh, Brij B. Gupta ,” Distributed Denial-of-Service (DDoS) Attacks and Defense Mechanisms in Various Web-Enabled Computing Platforms: Issues, Challenges, and Future Research Directions” , International Journal on Semantic Web and Information Systems, April 2022.

[4]Boyang Zhang, Zhang Tao, Zhijian Yu”, DDoS detection and prevention based on artificial intelligence techniques” , 1 December 2017 ,Computer Science, Engineering , 2017 3rd IEEE International Conference on Computer and Communications (ICCC)

[5]Yang, H.; He, X.; Wang, Z.; Qiu, R.C” Blind False Data Injection Attacks Against State Estimation Based on Matrix Reconstruction”, IEEE Trans. Smart Grid 2022, 7, 3174–3187.

[6]Vinicius, D.; Pedro, R.; Damien, M. Mario” Detection and Mitigation of Low-Rate Denial-of-Service Attacks”: A Survey. IEEE Access 2022, 10, 76648–76668.

[7]Kaur, S.; Kumar, K.; Aggarwal, N.; Singh, G. “A comprehensive survey of DDoS defense solutions in SDN: Taxonomy, research challenges, and future directions” Comput. Secur. 2021, 110, 102423.
[8]Yuan, J.; Mills, K. “Monitoring the macroscopic effect of DDoS flooding attacks”, IEEE Trans. Dependable Secur. Comput. 2005, 2, 324–335.
[9]Biswas, R.; Kim, S.; Wu, J. Sampling Rate Distribution for Flow Monitoring and DDoS Detection in Datacenter. IEEE Trans. Inf. Forensics Secur. 2021, 16, 2524–2534.
[10] Tsobdjou, L.D.; Pierre, S.; Quintero, A. “An Online Entropy-Based DDoS Flooding Attack Detection System with Dynamic Threshold.” IEEE Trans. Netw. Serv. Manag. 2022, 19, 1679–1689.
[11] Li, R.; Wu, B. “Early detection of DDoS based on φ-entropy in SDN networks”. In Proceedings of the 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)”, Darmstadt, Germany, 12–14 June 2020; pp. 731–735.
[12] Ahalawat, A.; Babu, K.S.; Turuk, A.K.; Patel, S. “A low-rate DDoS detection and mitigation for SDN using Renyi Entropy with Packet Drop” , J. Inf. Secur. Appl. 2022,

