EduVision: Journal of Innovations in Pedagogy and Educational Advancements
Volume 2, Issue 2, February 2026
brightmindpublishing.com
ISSN (E): 3061-6972
Licensed under* CC BY 4.0 *a Creative Commons Attribution 4.0 International License.

DDOS ATTACKS AND MODERN PROTECTION MECHANISMS

G. J. Ergashev 1,
1 PhD. International Islamic Academy of Uzbekistan
E-mail:giyosjonergashev23@gmail.com

F. K. Islamova 2
2Tashkent Institute of Chemical Technology

Abstract
The development of modern information technologies and the global Internet has made information security issues increasingly relevant.
DDoS attacks pose a threat to network infrastructure and service availability.
These attacks, directed at networks and existing systems, can slow down system performance or completely stop it. Technologies such as Cloudflare, AWS Elastic Load Balancing, WAF, and DeepDefend are effective tools for detecting ongoing attacks and preventing their consequences. An integrated approach ensures the stable operation of multiple systems and applications.

Keywords: DDoS attacks, availability, Cloudflare, Load Balancing, WAF (Web Application Firewall), DeepDefend, AWS Elastic Load Balancing (ELB).

Introduction

The rapid development of information and communication technologies, the widespread implementation of cloud computing, the Internet of Things (IoT), 5G networks, and digital platforms are transforming the global information infrastructure into a complex and interconnected ecosystem.
Although this transformation has increased economic efficiency, speed, and service scalability, it has simultaneously generated a new spectrum of cybersecurity threats.In particular, Distributed Denial of Service (DDoS) attacks targeting the principle of service availability have become one of the most pressing issues in the modern cybersecurity environment.
DDoS attacks are essentially aimed at disabling the resources of a targeted server, network, or application by sending an extremely large volume of artificial traffic,

EduVision: Journal of Innovations in Pedagogy and Educational Advancements
Volume 2, Issue 2, February 2026
brightmindpublishing.com
ISSN (E): 3061-6972
Licensed under CC BY 4.0 *a Creative Commons Attribution 4.0 International License.*

including CPU power, RAM, and network bandwidth.In particular, DDoS attacks pose a direct threat to network infrastructure and service availability. DDoS attacks remain one of the primary risk factors for online services and infrastructures. They are rapidly becoming more sophisticated and are capable of bypassing traditional detection mechanisms.

Such developments require an in-depth analysis of current attack trends and the effectiveness of detection strategies. DDoS attacks overload networks, causing systems to slow down or completely stop functioning, thereby creating significant information security problems. This type of attack not only enables unauthorized users to access services but also restricts legitimate users from using them. Today, models such as DeepDefend, as well as services like Cloudflare and Load Balancing, play an important role in effectively combating such attacks. To mitigate DDoS attacks and reduce their risks, modern solutions such as Cloudflare, Load Balancing, and many other technologies are widely used. Below, we analyze the role and importance of Cloudflare and Load Balancing technologies.

DDoS attacks are carried out by sending malicious traffic to a network or system. Attackers use multiple compromised systems or botnets to overload the network with excessive requests, resulting in system slowdown or complete failure. DDoS attacks are generally divided into three categories: Network (Volumetric) attacks, Protocol attacks, and Application Layer attacks.

Network attacks aim to saturate bandwidth with massive traffic. Protocol attacks exploit vulnerabilities in network protocols.

Application Layer attacks target weaknesses in higher layers of the system. Several technologies are effectively used to combat DDoS attacks. One of the most effective methods is Load Balancing technology. By distributing traffic across multiple servers, system stability can be ensured. This technology plays a crucial role in network optimization and security enhancement.

Services such as Cloudflare provide protective mechanisms against DDoS attacks. Cloudflare provides global network security and optimization services. Its primary function is to combat DDoS attacks, protect systems, and optimize traffic.

EduVision: Journal of Innovations in Pedagogy and Educational Advancements
Volume 2, Issue 2, February 2026
brightmindpublishing.com
ISSN (E): 3061-6972
Licensed under **CC BY 4.0** *a Creative Commons Attribution 4.0 International License.*

Cloudflare offers the following capabilities:

1.Global Load Balancing: Distributes traffic through a global network of servers to ensure system stability and prevent DDoS attacks.

2.Bot Management: Detects and blocks malicious bots to protect systems.

3.Traffic Filtering: Analyzes incoming requests in real time and automatically blocks malicious traffic.

4.Content Delivery Network (CDN): Ensures fast content delivery and helps mitigate DDoS attacks through a global CDN infrastructure. Load Balancing technology ensures system stability by efficiently distributing traffic across servers.

By distributing traffic among servers, the system is protected from overload and the impact of DDoS attacks is reduced.The main Load Balancing methods include:

1. Round-robin: Evenly distributes traffic requests across all servers.

2. Least connections: Directs traffic to the server with the fewest active connections.

3.IP Hashing: Distributes traffic based on the user's IP address.

Load Balancing technology effectively helps reduce the impact of DDoS attacks. If excessive malicious traffic is sent to one server, requests are automatically redirected to other servers, ensuring continuous system operation. As a practical example, Amazon Web Services (AWS) Elastic Load Balancing can be mentioned.

Amazon Web Services (AWS) provides the Elastic Load Balancing (ELB) service, which is widely used to optimize and secure networks. AWS ELB distributes traffic across multiple servers and data centers, helping to prevent DDoS attacks.

Load balancing includes the following types:

1. Application Load Balancer (ALB): Designed for high-level protocols, particularly HTTP/HTTPS.

2. Network Load Balancer (NLB): Provides high-performance and low-latency distribution for network protocols.

3. Classic Load Balancer (CLB): Based on earlier AWS services and intended for general-purpose use.

EduVision: Journal of Innovations in Pedagogy and Educational Advancements
Volume 2, Issue 2, February 2026
brightmindpublishing.com
ISSN (E): 3061-6972
Licensed under **CC BY 4.0** *a Creative Commons Attribution 4.0 International License.*

Compared to Cloudflare, AWS Elastic Load Balancing offers advantages in terms of flexible integration tailored to specific user needs.
At the same time, AWS services have a broad network of global data centers, ensuring higher efficiency in delivering services worldwide.

Conclusion

DDoS attacks pose a significant threat to information security today. To detect and mitigate DDoS attacks, a multi-layered architecture is required, including edge providers such as Cloudflare, global and application-level load balancing, WAF (Web Application Firewall), and DeepDefend. Technical integration, real-time monitoring, automated mitigation processes, and regular updates are fundamental principles.
Technologies such as Cloudflare and AWS Elastic Load Balancing are among the key tools in combating these attacks.
Load balancing is not a standalone protection mechanism but a component of a comprehensive security strategy.
When combined with other tools, it achieves maximum effectiveness. Cloudflare's global security services and AWS ELB's integrated load balancing services optimize networks and effectively detect malicious traffic. These mechanisms enable systems to withstand attacks while maintaining uninterrupted service delivery to legitimate users.

References

1. Jincheng Wang, Le Yu, John C. S. Lui, Xiapu Luo.Modern DDoS Threats and Countermeasures: Insights into Emerging Attacks and Detection Strategies.2025.
2.Mohamed Ouhssini, Karim Afdel, Elhafed Agherrabi, Mohamed Akouhar, Abdallah Abarda. Computer and Information Sciences.Journal of King Saud University. 2024.
3.Jahangir Shaikh,Toqeer Ali Syed,Syed Aziz Shah,Salman Jan,Curat Ul Ain and Pradeep Kumar Singh. Advancing DDoS attack detection with hybrid deep learning: integrating convolutional neural networks, PCA, and vision transformers.International Journal on Smart Sensing and Intelligent Systems, 2024.