# *Denial of Service (DoS)*

*200007626*
*CS5020 P1*

*12/10/2023*

*School of Computer Science*
*University of St. Andrews*

# Index of Sections

## I. Introduction

In 2020, the global production and consumption of data was over thirty times higher than that of 2010, reaching 64.2 zettabytes – that's 64.2 trillion gigabytes [1]. By 2025, the figure is predicted nearly three times higher, at 181 zettabytes [1]. The 21st century has been a period of tremendous growth for the amount of data and information we can generate and consume; the value of the 'Big Data' analytics industry, which "(examines) and (analyses) massive and varied data … (to) help organisations make more-informed business decisions" [2, p. 1], is forecast to surpass 655 billion USD by 2029 [3]. In some cases, we are involved in the production of this data, like when we decide to upload an image to a social media service, backup our information to cloud services, or send an email using an email service provider. However, most of us are primarily consumers of data, constantly making requests for content over networks through media streaming services, internet browsers, and news sources [4]. As of July 2023, 64.5% of the world's population was connected to the Internet [5] – this group of people may have learned to rely on banking, communication, and entertainment services provided online. Microcontrollers within modern cars are communicated with using "unidirectional Radio Frequency transmission" to allow "Remote Keyless Entry" [6]. Even our access to electricity from an energy grid now relies on "cyber-physical systems" and "communication technologies" to enable "smart distribution, generation, and storage of energy" [7, p. 1]. Our societal and individual dependence on network connections and services is the very reason why Denial of Service (DoS) Attacks can be so devastating.

First deployed in 1996 to disrupt the Internet Service Provider (ISP) 'Panix' [8], a DoS attack is "a class of cyber attacks designed to render a service inaccessible" [9, Sec. 1]. In the case of the attack against Panix, the hacker exploited an aspect of the TCP protocol to perform a resource-depleting 'SYN flood' attack [8], [10]. Over time, the technologies and procedures involved in a DoS attack have evolved, but the goal of the attack has remained the same. Attackers' motivations can vary dramatically, with some wanting to gain respect, to show off, or simply to have fun. Others have more concrete motivations: some political, some ethical, and some financial [11] - nearly a third of enterprises worldwide experienced some form of a DoS attack in 2020 [12]. Before delving into specific examples of DoS attacks and mitigation techniques, we will first provide an overview of the various classes of DoS attacks from a functionality perspective.

## II. Technical Discussion

DoS attacks can be classified using a variety of qualifiers and perspectives – for example, [13, pp. 3663–3664] considers the result of an attack to be its defining feature, citing bandwidth consumption, resource consumption, and web server failure. Reference [14, pp. 2048–2050] instead classifies attacks according to the protocol level that is targeted, separating network and transport-level approaches from application-level attacks. Considering DoS attacks based on their impact on network services, [15, p. 191] provides perhaps the simplest and most apt classification split, separating attacks into two simple categories: bandwidth depletion, and resource depletion. It is worth nothing that while both types of attacks will consume bandwidth and resources to varying degrees, bandwidth depletion attacks (BDA) are used most effectively when the weakest point in a network is the bandwidth of the network link, rather than the processing power of individual end-points on the network; similarly, resource depletion attacks (RDA) will be most effective in the converse scenario, where the bandwidth of a network is very large, but the processing power of end-points in the network are comparatively low.

### A. *Bandwidth Depletion Attacks (BDA)*

Bandwidth depletion attacks "seek to consume the available bandwidth or router resources at or near a target host or network, such that legitimate traffic cannot reach its destination" – they "saturate network links", causing blockages or traffic jams on the network. [16, p. 836]. To reduce the number of instances of network traffic congestion, many networking and communication protocols implement congestion controls, such as the 'Bottleneck Bandwidth and Round-trip propagation time' algorithm discussed in [17]. Attempting to perform bandwidth depletion attacks using these protocols can therefore be difficult, since transmission rates will automatically be reduced as the bandwidth capacity limit of the victim's network is approached. However, there are many protocols that make no attempt to implement such congestion controls, such as the User Datagram Protocol (UDP) [18] and the Internet Control Message Protocol (ICMP) [19].

The ICMP is a "message protocol that is … used to report any problems in the network, … (and to) get specific information from a router or host in the network" [20, p. 124]. Considering how this protocol might be used in a DoS attack, there is a specific message implemented using ICMP called an 'echo request', more commonly known as a 'ping'. The ICMP echo-request is sent to a specific IP address, and results in the target machine sending an 'echo reply' message to the IP address of origin. While legitimate users of these requests will be interested in the data contained in the messages, such as packet loss and round-trip time, attackers are not concerned with the content of these packets. Rather, the attacker appreciates that a very high volume of these messages can be sent through a network due to their lack of congestion control, and will deplete the bandwidth of a network completely at a given volume. Moreover, this attack generates both in-bound and out-bound traffic across a given network, ensuring congestion of both channels. Known as a 'Ping flood' [21], this attack is one of many different approaches attackers can use to deplete the bandwidth of a network. Due to the requirement of a high volume of messages for efficacy, modern BDAs often make use of 'botnets' [22, Sec. 1.1] constructed with various compromised machines to distribute their DoS attack – using multiple machines not only increases the maximum number of messages that can be sent at any one time, but also provides distributed anonymity to the attacker, making it harder to identify and block the attack source.

### B. *Resource Depletion Attacks (RDA)*

If a target network has high levels of bandwidth, but comparatively low levels of computational power in its endpoints, depleting the resources of these machines is another viable method used to deny service. RDAs are "designed to tie up the resources of a victim system" [15, p. 191], and can produce different results depending on the targeted endpoint. For example, if a server containing important documentation within a business network is targeted, employees might not be able to access these documents, but will still be able to communicate over the network, as their personal machines have not been attacked. Alternatively, if a router or switch within a network is targeted, all users of the network might experience downtime and denial of service from the router as a result of its computational resources having been exhausted.

In keeping with the previous example, it is possible to carry out an RDA using the ICMP – this time, instead of relying on the volume of packets we can send through a network, we instead focus on the content of a single packet. Known as the 'Ping of Death', this attack involves "sending a packet larger than the maximum allowable size, causing the target machine to freeze or crash" [23]. When packets are to be sent over a network link, the link will have a maximum transmission unit (MTU) – if a packet is larger than the limit allowed by the network link, it is fragmented at the source, transmitted, and reassembled at the destination [24, p. 25]. As the IPv6 specification notes, some systems are not capable of reassembling larger packets [24, p. 25] due to buffer limitations [23]. If large packets are sent to systems incapable of carrying out the reassembly to completion, a buffer overflow can occur, "causing the target machine to freeze, crash, or reboot" [23, Sec. 2]. As Cloudflare notes, this attack is now mostly obsolete against devices created after 1998 [23, Sec. 3], as systems will monitor the reassembly process to ensure a buffer overflow does not occur. However, it is perhaps one of the most famous RDAs, and serves to emphasise that RDAs are based on exploiting specific protocols, procedures, and interactions, rather than on volume of data transmission alone.

## III. Types and Impact of DoS Attacks

To discuss the various types of DoS attacks most effectively, we can make further distinctions within the two classes we have defined. Within the BDA category, [25, Fig. 5] notes that there are two main attack mechanisms employed, with attacks either preferring to use protocol exploits, or attempting to amplify the volume of traffic sent to a target using IP spoofing and asymmetric requests. The RDA category likewise has two main subcategories: protocol exploits, and malformed packets. The following is a brief description of a few specific attacks that implement these mechanisms, and their effect on network services.

### A. *Protocol Exploit (BDA)*

As discussed previously, attacks can exploit the absence of congestion controls within the ICM Protocol to send massive volumes of data to a network, causing traffic congestion and bandwidth depletion for all endpoints involved. A similar process is possible using the UDP [18], another connectionless messaging protocol, with attackers usually spoofing their IP addresses to avoid traceability, and having to deal with the packets returned by the victim [26, Sec. 1]. The attacker creates a UDP packet with a spoofed IP origin address, and sends this packet to a device in the target network, specifying an IP address and a port number. When the device on the network receives this packet, it checks if any programs are currently listening for messages on the specified port number – most often, this will not be the case. As a result, this endpoint within the network returns an ICMP error message to what it believes to be the sender – but in actuality, was a random IP address used to hide or 'spoof' the attacker's true location and identity. Similarly to ICMP flooding, modern attacks involve the use of many attacking machines in the form of botnets, to ensure an adequate volume of UDP packets are sent to the victim network in order to cause bandwidth depletion [26].

### B. *Amplification (BDA)*

While simply sending data directly to a network can be effective given a large enough botnet, attackers can utilise reflection techniques to increase the volume of traffic sent to their target by multiple orders of magnitude. To understand the mechanisms used in perhaps the most common type of amplification attack, it is important to first cover Domain Name System (DNS) resolvers – these open resolvers can be communicated with by anyone, and are used to convert names of domains, such as 'Google.com', into IP addresses. These open DNS resolvers are extremely important to the overall functionality of the Internet, but attackers can use these resolvers to greatly amplify the volume of traffic used in their attack. By creating requests for large amounts of information, and spoofing the IP address of the target network, these requests result in a large amount of traffic from DNS resolvers being sent to the victim [27]. These attacks can have devastating effects on the availability of a network when performed by a botnet utilising multiple DNS resolvers at once, with previous historical attacks reaching transmission rates of around and above two terabits per second [28], [29, Sec. 3]. Similar attacks are possible using the Network Time Protocol (NTP), used "by hundreds of millions of computers and devices to synchronise their clocks over the internet" [30]. By passing the command 'monlist' to servers which implement the NTP, a response containing a list of  the last 600 devices that communicated with the server is sent to the victim [31, Sec. 1].

### C. *Protocol Exploit (RDA)*

Unlike its connectionless counterpart, the Transmission Control Protocol (TCP) is a connection-based communication protocol, and involves a three-way handshake procedure to establish connections [32]. This protocol can be exploited by attackers in order to consume resources of specific servers on a network, in what is known as a 'SYN flood' [33]. To initiate a communication channel using TCP, a sync request (SYN) is sent to the target machine using their IP address – this machine then reads the SYN packet, responds with a sync acknowledgement (SYN ACK), and waits for a corresponding acknowledgement (ACK) from the machine that initiated the request. Under normal circumstances, the machine that wishes to establish a connection reads this acknowledgement, sends a final acknowledgement to the target machine, and a communication channel is assigned for both machines. In a SYN flood attack however, an attacker sends a SYN packet with a spoofed IP address, and has no intention of responding with a final acknowledgement. This leaves the target machine waiting for a message they will never receive, and causes the server to dedicate resources to holding the potential connections in its connection table [10, Sec. 5], leaving normal traffic unable to connect to the server and access the network-based services.

An alternative and perhaps more subtle approach is termed the 'Slowlorris' attack, whereby attackers complete TCP connections as intended, and then begin to send "partial HTTP requests at regular intervals" [34, Sec. 2 C]. These requests will in actuality never be sent in completion, and results in the server holding multiple concurrent connections open until it is no longer capable of forming any more, resulting in a denial of service for genuine users. This attack is difficult to detect, as it involves sending valid HTTP requests that resemble normal traffic, and is but one of the many techniques that form a further subcategory of attacks know as 'Low and Slow' [34].

### *D. Malformed Packet (RDA)*

Finally, much like the historic 'Ping of Death' [23], malformed packet attacks are intended to cause the victim's system to respond in an unexpected fashion – an additional example in this category of attacks is known as the 'LAND attack' (Local Area Network Denial) [35, Sec. 2.1]. This attack involves designing a TCP packet with a spoofed IP source and address, both of which belong to the target server. When the victim's server receives this packet, it attempts to reply to itself, and enters "an infinite loop because of identical source and destination address, causing a crash in (the) victim's machine" [35, Sec. 2.1]. There are many other known attacks that belong to this subcategory [36, Sec. 3.2.2], and many further 'Zero Day' attacks that currently have no known mitigation techniques.

## IV. Mitigation Strategies

Both Kukreti et al. [33, Sec. 2 C] and Cloudflare [37] identify the following four stages of mitigating Denial of Service attacks: discovery, filtering, routing, and adaptation – there are many recognised techniques networks can deploy within each stage.

There have been several behaviour-based machine learning models and algorithms developed to detect and differentiate high levels of traffic from a DoS attack [38]–[40], including 'Random Forest; and 'Naïve Bayes', 'Multi-layer Perceptron', and 'J48 (C4.5)' classifiers [39, Sec. 4]. These models are highly effective compared to simpler inline packet-level firewall detection methods, as they are capable of identifying subtle differences in traffic flow in ways that rule-based systems are not.

Once malicious traffic has been identified, targeted systems will wish to filter out and drop these packets to minimise their effect on the network. Web application firewalls that employ 'Deep Learning' principles [41] can be effectively used to prevent DoS against application-level attacks, and rate-limiting the attack traffic is another viable approach [42].

Intelligent routing can "help collapse the outstanding traffic into untroublesome segments" [33, Sec. 2 C], especially if attacks are solely volume-based. Virtually distributed networks can distribute content to various servers, "(sharing) the pressure" of an attack [43, Sec. 2.1]; additionally, 'load balancing techniques' can be used to route traffic with an even distribution between these servers, with existing algorithms including the 'Round-Robin', 'Ant colony optimization', and 'Two-step load balancing' [44, Tbl. 1]. Malformed packets can be differently dealt with by simply dropping them, known as 'Blackhole routing'.

Lastly, the adaptation phase of the mitigation process often occurs after an attack has taken place, and involves "(analysing) the common pattern followed by an attacker" [33, Sec. 2 C]. Behavioural detection models may be trained on logs recorded during an attack; specific system vulnerabilities to malformed packets may be identified and resolved; redistribution of network services and resources may be necessary; and identifying and blocking attackers' IP addresses is best practice if possible.

## V. Conclusion

There are an ever-changing number of exploits, methodologies, and techniques utilisable by attackers to cause Denial of Service for networks and endpoints, as well as an increasing number of mitigation techniques against these attacks. Attacks can be categorised by their intended effect on the network, and these categories can be further split by their method of attack. In response to a DoS attack, networks and services can make use of the widely-accepted [33, 37] four-step response procedure to detect, filter, route, and adapt to attacks, and ensure that they continue to provide service to intended users of their systems.

## Bibliography

[1] P. Taylor, 'Data growth worldwide 2010-2025', Statista. Accessed: Oct. 11, 2023. [Online]. Available: https://www.statista.com/statistics/871513/worldwide-data-created/

[2] A. H. Gandomi, F. Chen, and L. Abualigah, 'Machine Learning Technologies for Big Data Analytics', Electronics, vol. 11, no. 3, p. 421, Jan. 2022, doi: 10.3390/electronics11030421.

[3] P. Taylor, 'Topic: Big data', Statista. Accessed: Oct. 11, 2023. [Online]. Available: https://www.statista.com/topics/1464/big-data/

[4] A. Petrosyan, 'Reasons for using the internet worldwide 2023', Statista. Accessed: Oct. 11, 2023. [Online]. Available: https://www.statista.com/statistics/1387375/internet-using-global-reasons/

[5] A. Petrosyan, 'Countries with the highest internet penetration rate 2023', Statista. Accessed: Oct. 11, 2023. [Online]. Available: https://www.statista.com/statistics/227082/countries-with-the-highest-internet-penetration-rate/

[6] R. P. Parameswarath and B. Sikdar, 'An Authentication Mechanism for Remote Keyless Entry Systems in Cars to Prevent Replay and RollJam Attacks', in 2022 IEEE Intelligent Vehicles Symposium (IV), Aachen, Germany: IEEE, Jun. 2022, pp. 1725–1730. doi: 10.1109/IV51971.2022.9827256.

[7] I. Ortega-Fernandez and F. Liberati, 'A Review of Denial of Service Attack and Mitigation in the Smart Grid Using Reinforcement Learning', Energies, vol. 16, no. 2, p. 635, Jan. 2023, doi: 10.3390/en16020635.

[8] R. E. Calem, 'New York's Panix Service Is Crippled by Hacker Attack', New York Times. Accessed: Sep. 26, 2023. [Online]. Available: https://archive.nytimes.com/www.nytimes.com/library/cyber/week/0914panix.html

[9] NCSQ UK, 'Denial of Service (DoS) guidance', Denial of Service (DoS) guidance. Accessed: Sep. 26, 2023. [Online]. Available: https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection

[10] M. Dulik, 'Network attack using TCP protocol for performing DoS and DDoS attacks', in 2019 Communication and Information Technologies (KIT), Vysoke Tatry, Slovakia: IEEE, Oct. 2019, pp. 1–6. doi: 10.23919/KIT.2019.8883481.

[11] A. Singh and B. B. Gupta, 'Distributed Denial-of-Service (DDoS) Attacks and Defense Mechanisms in Various Web-Enabled Computing Platforms: Issues, Challenges, and Future Research Directions', Int. J. Semantic Web Inf. Syst. IJSWIS, vol. 18, no. 1, pp. 1–43, 2022, doi: 10.4018/IJSWIS.297143.

[12] Statista Research Department, 'Enterprise IT threats and concerns worldwide 2020', Statista. Accessed: Oct. 11, 2023. [Online]. Available: https://www.statista.com/statistics/1229539/enterprise-it-threat-and-concerns-by-category/

[13] B. B. Gupta and O. P. Badve, 'Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a Cloud computing environment', Neural Comput. Appl., vol. 28, no. 12, pp. 3655–3682, Dec. 2017, doi: 10.1007/s00521-016-2317-5.

[14] S. T. Zargar, J. Joshi, and D. Tipper, 'A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks', IEEE Commun. Surv. Tutor., vol. 15, no. 4, pp. 2046–2069, 2013, doi: 10.1109/SURV.2013.031413.00127.

[15] C. Douligeris and A. Mitrokotsa, ‘DDoS attacks and defense mechanisms: a classification’, in Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology (IEEE Cat. No.03EX795), Dec. 2003, pp. 190–193. doi: 10.1109/ISSPIT.2003.1341092.

[16] A. D. Keromytis, ‘Network Bandwidth Denial of Service (DoS)’, in Encyclopedia of Cryptography and Security, H. C. A. Van Tilborg and S. Jajodia, Eds., Boston, MA: Springer US, 2011, pp. 836–838. doi: 10.1007/978-1-4419-5906-5_271.

[17] N. Cardwell, Y. Cheng, C. S. Gunn, S. H. Yeganeh, and Van Jacobson, ‘BBR: congestion-based congestion control’, Commun. ACM, vol. 60, no. 2, pp. 58–66, Jan. 2017, doi: 10.1145/3009824.

[18] RFC, ‘User Datagram Protocol’, Internet Engineering Task Force, Request for Comments RFC 768, Aug. 1980. Accessed: Oct. 11, 2023. [Online]. Available: https://datatracker.ietf.org/doc/rfc768/

[19] RFC, ‘Internet Control Message Protocol’, Internet Engineering Task Force, Request for Comments RFC 792, Sep. 1981. Accessed: Oct. 11, 2023. [Online]. Available: https://datatracker.ietf.org/doc/rfc792/

[20] R. B. Junior and S. Kumar, ‘Apple’s Lion vs Microsoft’s Windows 7: Comparing Built-In Protection against ICMP Flood Attacks’, J. Inf. Secur., vol. 2014, Jun. 2014, doi: 10.4236/jis.2014.53012.

[21] Cloudflare, ‘Ping (ICMP) flood DDoS attack’, Ping (ICMP) flood DDoS attack. Accessed: Oct. 11, 2023. [Online]. Available: https://www.cloudflare.com/en-gb/learning/ddos/ping-icmp-flood-ddos-attack/

[22] D. Georgoulias, J. M. Pedersen, M. Falch, and E. Vasilomanolakis, ‘Botnet Business Models, Takedown Attempts, and the Darkweb Market: A Survey’, ACM Comput. Surv., vol. 55, no. 11, pp. 1–39, Nov. 2023, doi: 10.1145/3575808.

[23] Cloudflare, ‘Ping of death DDoS attack’, Ping of death DDoS attack. Accessed: Oct. 11, 2023. [Online]. Available: https://www.cloudflare.com/en-gb/learning/ddos/ping-of-death-ddos-attack/

[24] S. E. Deering and B. Hinden, ‘Internet Protocol, Version 6 (IPv6) Specification’, Internet Engineering Task Force, Request for Comments RFC 8200, Jul. 2017. Accessed: Oct. 11, 2023. [Online]. Available: https://datatracker.ietf.org/doc/rfc8200/

[25] T. Mahjabin, Y. Xiao, G. Sun, and W. Jiang, ‘A survey of distributed denial-of-service attack, prevention, and mitigation techniques’, Int. J. Distrib. Sens. Netw., vol. 13, no. 12, p. 155014771774146, Dec. 2017, doi: 10.1177/1550147717741463.

[26] Cloudflare, ‘UDP flood attack’, UDP flood attack. Accessed: Oct. 12, 2023. [Online]. Available: https://www.cloudflare.com/en-gb/learning/ddos/udp-flood-ddos-attack/

[27] Cloudflare, ‘DNS amplification attack’, DNS amplification attack. Accessed: Oct. 12, 2023. [Online]. Available: https://www.cloudflare.com/en-gb/learning/ddos/dns-amplification-ddos-attack/

[28] O. Yoachimik, ‘Cloudflare blocks an almost 2 Tbps multi-vector DDoS attack’, The Cloudflare Blog. Accessed: Oct. 12, 2023. [Online]. Available: http://blog.cloudflare.com/cloudflare-blocks-an-almost-2-tbps-multi-vector-ddos-attack/

[29] D. Menscher, ‘Identifying and protecting against the largest DDoS attacks’, Google Cloud Blog. Accessed: Oct. 12, 2023. [Online]. Available: https://cloud.google.com/blog/products/identity-security/identifying-and-protecting-against-the-largest-ddos-attacks

[30] Google, ‘Public NTP’, Google for Developers. Accessed: Oct. 12, 2023. [Online]. Available: https://developers.google.com/time

[31] J. Czyz, M. Kallitsis, M. Gharaibeh, C. Papadopoulos, M. Bailey, and M. Karir, ‘Taming the 800 Pound Gorilla: The Rise and Decline of NTP DDoS Attacks’, in Proceedings of the 2014 Conference on Internet Measurement Conference, Vancouver BC Canada: ACM, Nov. 2014, pp. 435–448. doi: 10.1145/2663716.2663717.

[32] J. Postel, ‘Transmission Control Protocol’, RFC Editor, RFC0793, Sep. 1981. doi: 10.17487/rfc0793.

[33] S. Kukreti, S. K. Modgil, N. Gehlot, and V. Kumar, ‘DDoS Attack using SYN Flooding: A Case Study’, in 2022 9th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India: IEEE, Mar. 2022, pp. 323–329. doi: 10.23919/INDIACom54597.2022.9763108.

[34] A. N. H. D. Sai, B. H. Tilak, N. S. Sanjith, P. Suhas, and R. Sanjeetha, ‘Detection and Mitigation of Low and Slow DDoS attack in an SDN environment’, in 2022 International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics ( DISCOVER), Oct. 2022, pp. 106–111. doi: 10.1109/DISCOVER55800.2022.9974724.

[35] M. Balaji Bharatwaj, M. Aditya Reddy, T. Senthil Kumar, and S. Vajipayajula, ‘Detection of DoS and DDoS Attacks Using Hidden Markov Model’, in Inventive Communication and Computational Technologies, G. Ranganathan, X. Fernando, and F. Shi, Eds., in Lecture Notes in Networks and Systems. Singapore: Springer Nature, 2022, pp. 979–992. doi: 10.1007/978-981-16-5529-6_74.

[36] A. Gaurav, B. B. Gupta, W. Alhalabi, A. Visvizi, and Y. Asiri, ‘A comprehensive survey on DDoS attacks on various intelligent systems and it’s defense techniques’, Int. J. Intell. Syst., vol. 37, no. 12, pp. 11407–11431, Dec. 2022, doi: 10.1002/int.23048.

[37] Cloudflare, ‘What is DDoS mitigation?’, What is DDoS mitigation? Accessed: Oct. 12, 2023. [Online]. Available: https://www.cloudflare.com/en-gb/learning/ddos/ddos-mitigation/

[38] T. E. Ali, Y.-W. Chong, and S. Manickam, ‘Machine Learning Techniques to Detect a DDoS Attack in SDN: A Systematic Review’, Appl. Sci., vol. 13, no. 5, p. 3183, Jan. 2023, doi: 10.3390/app13053183.

[39] P. S. Saini, S. Behal, and S. Bhatia, ‘Detection of DDoS Attacks using Machine Learning Algorithms’, in 2020 7th International Conference on Computing for Sustainable Global Development (INDIACom), Mar. 2020, pp. 16–21. doi: 10.23919/INDIACom49435.2020.9083716.

[40] S. S. Priya, M. Sivaram, D. Yuvaraj, and A. Jayanthiladevi, ‘Machine Learning based DDOS Detection’, in 2020 International Conference on Emerging Smart Computing and Informatics (ESCI), Mar. 2020, pp. 234–237. doi: 10.1109/ESCI48226.2020.9167642.

[41] B. Dawadi, B. Adhikari, and D. Srivastava, ‘Deep Learning Technique-Enabled Web Application Firewall for the Detection of Web Attacks’, Sensors, vol. 23, no. 4, p. 2073, Feb. 2023, doi: 10.3390/s23042073.

[42] A. G. Alcoz, M. Strohmeier, V. Lenders, and L. Vanbever, ‘Aggregate-based congestion control for pulse-wave DDoS defense’, in Proceedings of the ACM SIGCOMM 2022 Conference, in SIGCOMM ’22. New York, NY, USA: Association for Computing Machinery, Aug. 2022, pp. 693–706. doi: 10.1145/3544216.3544263.

[43] Z. Li and W. Meng, ‘Mind the Amplification: Cracking Content Delivery Networks via DDoS Attacks’, in Wireless Algorithms, Systems, and Applications, vol. 12938, Z. Liu, F. Wu, and S. K. Das, Eds., Cham: Springer International Publishing, 2021, pp. 186–197. doi: 10.1007/978-3-030-86130-8_15.

[44] N. M. Abdulkareem and S. R. M. Zeebaree, ‘OPTIMIZATION OF LOAD BALANCING ALGORITHMS TO DEAL WITH DDOS ATTACKS USING WHALE OPTIMIZATION ALGORITHM’, J. Duhok Univ., vol. 25, no. 2, pp. 65–85, Nov. 2022, doi: 10.26682/sjuod.2022.25.2.7.

Word count: 2856