

DAFTAR PUSTAKA

- Arazi, E. (2017) *5 Questions to Ask About DDoS Pricing*, Radware Blog. Available at: <https://blog.radware.com/security/2017/11/5-questions-about-ddos-pricing/> (Accessed: 5 January 2022).
- Arazi, E. (2018) *Rate Limiting - A Cure Worse Than the Disease?*, Radware Blog. Available at: <https://blog.radware.com/security/2018/09/rate-limiting-a-cure-worse-than-the-disease/> (Accessed: 29 December 2021).
- Baldini, I., Castro, P., Chang, K., Cheng P., Fink, S., Ishakian, V., Mitchell, N., Muthusamy, V., Rabbahm, R., Slominski, A., and Suter, P. (2017) 'Serverless Computing: Current Trends and Open Problems', in S. Chaudhary, G. Somani, and R. Buyya (eds) *Research Advances in Cloud Computing*. Singapore: Springer Singapore, pp. 1–20. Available at: https://doi.org/10.1007/978-981-10-5026-8_1.
- Bengio, Y., Courville, A. and Vincent, P. (2013) 'Representation Learning: A Review and New Perspectives', *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 35(8), pp. 1798–1828. Available at: <https://doi.org/10.1109/TPAMI.2013.50>.
- Braden, R.T. (1989) *Requirements for Internet Hosts - Communication Layers*. Request for Comments RFC 1122. Internet Engineering Task Force. Available at: <https://doi.org/10.17487/RFC1122>.
- Calvert, C., Kemp, C., Khoshgoftaar, T., Najafabadi, M. (2019) 'Detecting Slow HTTP POST DoS Attacks Using Netflow Features', in *The Thirty-Second International Flairs Conference. The Thirty-Second International Flairs Conference*. Available at: <https://www.aaai.org/ocs/index.php/FLAIRS/FLAIRS19/paper/view/18318> (Accessed: 8 September 2021).
- CISA (2019) *Understanding Denial-of-Service Attacks*. Available at: <https://www.cisa.gov/uscert/ncas/tips/ST04-015> (Accessed: 24 December 2021).
- Cloudflare (2018a) *What is a denial-of-service (DoS) attack?*, Cloudflare. Available at: <https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/> (Accessed: 30 November 2021).
- Cloudflare (2018b) *What is a low and slow attack? Low and slow DDoS attack definition*, Cloudflare. Available at: <https://www.cloudflare.com/learning/ddos/ddos-low-and-slow-attack/> (Accessed: 30 November 2021).

- Cloudflare (2018c) *What is TCP/IP?*, Cloudflare. Available at: <https://www.cloudflare.com/learning/ddos/glossary/tcp-ip/> (Accessed: 29 October 2021).
- Deng, L. and Yu, D. (2014) 'Deep Learning: Methods and Applications', *Foundations and Trends® in Signal Processing*, 7(3–4), pp. 197–387. Available at: <https://doi.org/10.1561/20000000039>.
- Dhanapal, A. and Nithyanandam, P. (2019) 'The Slow HTTP Distributed Denial of Service Attack Detection in Cloud', *Scalable Computing: Practice and Experience*, 20, pp. 285–298. Available at: <https://doi.org/10.12694/scpe.v20i2.1501>.
- Faria, V.D., Gonçalves, J.A., Silva, C.A, Vieira, G.D., and Mascarenhas, D.M. (2020) 'SDToW: A Slowloris Detecting Tool for WMNs', *Information*. Available at: <https://doi.org/10.3390/info11120544>.
- Fawcett, T. (2006) 'An introduction to ROC analysis', *Pattern Recognition Letters*, 27(8), pp. 861–874. Available at: <https://doi.org/10.1016/j.patrec.2005.10.010>.
- Géron, A. (2019) *Hands-on Machine Learning with Scikit-Learn, Keras, and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems*. O'Reilly Media, Incorporated.
- Gholamalinezhad, H. and Khosravi, H. (2020) 'Pooling Methods in Deep Neural Networks, a Review', *arXiv:2009.07485 [cs]* [Preprint]. Available at: <http://arxiv.org/abs/2009.07485> (Accessed: 28 November 2021).
- Goodfellow, I., Bengio, Y. and Courville, A. (2016) *Deep Learning*, MIT Press. Cambridge, MA, USA: The MIT Press.
- Hirakawa, T., Ogura, K., Bista, B.B., and Takata, T. (2016) 'A Defense Method against Distributed Slow HTTP DoS Attack', in *2016 19th International Conference on Network-Based Information Systems (NBIS). 2016 19th International Conference on Network-Based Information Systems (NBIS)*, Ostrava, Czech Republic: IEEE, pp. 152–158. Available at: <https://doi.org/10.1109/NBIS.2016.58>.
- Hu, J., Niu, H., Carrasco, J., Lennox, B., and Arvin, F. (2020) 'Voronoi-Based Multi-Robot Autonomous Exploration in Unknown Environments via Deep Reinforcement Learning', *IEEE Transactions on Vehicular Technology*, 69(12), pp. 14413–14423. Available at: <https://doi.org/10.1109/TVT.2020.3034800>.
- Kelly, D., Glavin, F.G. and Barrett, E. (2021) 'Denial of wallet—Defining a looming threat to serverless computing', *Journal of Information Security*

and Applications, 60, p. 102843. Available at:
<https://doi.org/10.1016/j.jisa.2021.102843>.

Kiranyaz, S., Avci, O., Abdeljaber, O., Ince, T., Gabbouj, M., and Inman, D.J. (2019) '1D Convolutional Neural Networks and Applications: A Survey', *arXiv:1905.03554 [cs, eess]* [Preprint]. Available at:
<http://arxiv.org/abs/1905.03554> (Accessed: 28 November 2021).

Lima Filho, F.S., Silveira, F., Medeiros Brito Junior, A., Vargas-Solar, G., and Silveira, L.F. (2019) 'Smart Detection: An Online Approach for DoS/DDoS Attack Detection Using Machine Learning', *Secur. Commun. Netw.*, 2019(december), pp. 1–15. Available at:
<https://doi.org/10.1155/2019/1574749>.

Lopez, A.D., Mohan, A.P. and Nair, S. (2019) 'Network Traffic Behavioral Analytics for Detection of DDoS Attacks', *SMU Scholar*, 2(1), p. 14.

Madarie, R. (2017) 'Hackers' motivations: Testing Schwartz's theory of motivational types of values in a sample of hackers', *International Journal of Cyber Criminology*, 11, pp. 78–97. Available at:
<https://doi.org/10.5281/zenodo.495773>.

Microsoft (2016) *What is PaaS? Platform as a Service* | *Microsoft Azure*. Available at: <https://azure.microsoft.com/en-us/overview/what-is-paas/> (Accessed: 30 November 2021).

Mozilla (2016) *An overview of HTTP - HTTP* | *MDN, MDN Web Docs*. Available at: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Overview> (Accessed: 30 November 2021).

Nelson, R. (2015) *DDoS Mitigation - Using NGINX to Prevent DDoS Attacks, NGINX*. Available at: <https://www.nginx.com/blog/mitigating-ddos-attacks-with-nginx-and-nginx-plus/> (Accessed: 19 December 2021).

Nugraha, B. and Murthy, R.N. (2020) 'Deep Learning-based Slow DDoS Attack Detection in SDN-based Networks', in *2020 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN). 2020 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, Leganes, Spain: IEEE, pp. 51–56. Available at:
<https://doi.org/10.1109/NFV-SDN50289.2020.9289894>.

Palmer, D. (2020) *DDoS attacks are cheaper and easier to carry out than ever before, ZDNet*. Available at: <https://www.zdnet.com/article/ddos-attacks-are-cheaper-and-easier-to-carry-out-than-ever-before/> (Accessed: 25 December 2021).

- Sambangi, S. and Gondi, L. (2020) 'A Machine Learning Approach for DDoS (Distributed Denial of Service) Attack Detection Using Multiple Linear Regression', *Proceedings*, 63(1), p. 51. Available at: <https://doi.org/10.3390/proceedings2020063051>.
- Shurman, M., Khrais, R. and Yateem, A.R. (2020) 'DoS and DDoS Attack Detection Using Deep Learning and IDS', *International Arab Journal of Information Technology*, 17, pp. 655–661. Available at: <https://doi.org/10.34028/iajit/17/4A/10>.
- Wang, D., Chen, X., Wang, Q., Wang, S., Xu, F., and Zheng, T. (2022) 'Autoscaling cracker: an efficient asymmetric DDoS attack on serverless functions', in *GLOBECOM 2022 - 2022 IEEE Global Communications Conference*, pp. 4179–4184. Available at: <https://doi.org/10.1109/GLOBECOM48099.2022.10001386>.
- Yeung, T. and Salsburg, D. (2018) *Do Web Hosts Protect Their Small Business Customers With Secure Hosting And Anti-Phishing Technologies?* Federal Trade Commission: Division of Litigation Technology & Analysis. Available at: https://www.ftc.gov/system/files/documents/reports/do-web-hosts-protect-their-small-business-customers-secure-hosting-anti-phishing-technologies/small_business_web_hosting_study_2-20-2018.pdf (Accessed: 30 December 2021).
- Zhang, M., Zhang, W. and Fan, K. (2012) 'Application Layer DDoS Detection Model Based on Data Flow Aggregation and Evaluation', in M. Zhao and J. Sha (eds) *Communications and Information Processing*. Berlin, Heidelberg: Springer Berlin Heidelberg (Communications in Computer and Information Science), pp. 37–45. Available at: https://doi.org/10.1007/978-3-642-31968-6_5.