REFERENCES

[1] M. Husák, J. Komárková, E. Bou-Harb, and P. Čeleda, "Survey of attack projection, prediction, and forecasting in cyber security," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 1, pp. 640–660, 2019.

[2] M. T. Manavi, "Defense mechanisms against Distributed Denial of Service attacks: A survey," *Computers and Electrical Engineering*, vol. 72, pp. 26–38, 2018. [Online]. Available: www.google.com

[3] M. Prince, "Empty DDoS Threats: Meet the Armada Collective," *CloudFlare*, 2016. [Online]. Available: https://blog.cloudflare.com/empty-ddos-threats-meet-the-armada-collective/

[4] Catalin Cimpanu, "Protocol used by 630,000 devices can be abused for devastating DDoS attacks | ZDNet," 2019. [Online]. Available: https://www.zdnet.com/article/protocol-used-by-630000-devices-can-be-abused-for-devastating-ddos-attacks/

[5] Arbor NETSCOUT, "Threat Intelligence Report -Powered by ATLAS Findings from First Half 2019," pp. 1–33, 2019. [Online]. Available: https://www.netscout.com/sites/default/files/2019-07/SECR{_}010{_}EN-1901\T1\textendashNETSCOUTThreatReport1H2019\T1\textendashWeb.pdf

[6] Akamai, "State of the Internet / Security Report | Credential Stuffing in the Media Industry," 2020. [Online]. Available: https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-credential-stuffing-in-the-media-industry-report-2020.pdf

[7] S. Ali and Y. Li, "Learning multilevel auto-encoders for ddos attack detection in smart grid network," *IEEE Access*, 2019.

[8] Y. Tsuge and H. Tanaka, "Quantification for Intrusion Detection System Using Discrete Fourier Transform," in *2016 International Conference on Information Science and Security (ICISS)*. IEEE, dec 2016, pp. 1–6. [Online]. Available: http://ieeexplore.ieee.org/document/7885867/

[9] M. Martellini and A. Malizia, *Cyber and Chemical, Biological, Radiological, Nuclear, Explosives Challenges: Threats and Counter Efforts*, 2017. [Online]. Available: https://books.google.co.id/books?id=klE8DwAAQBAJ{&}vq=siem+alarm+filtering{&}source=gbs{_}navlinks{_}shttps://books.google.com/books?id=klE8DwAAQBAJ{&}lpg=PA31{&}dq=siemalarmfiltering{&}pg=PA31{#}v=onepage{&}q=siemalarmfiltering{&}f=false

[10] S. Axelsson, "Intrusion Detection Systems: A Survey and Taxonomy [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.1.6603. [Accessed: 30-Sep- 2016]. [16]," *Technical Report*, vol. 99, pp. 1–15, 2000. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.1.6603

[11] K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," *National Institute of Standards and Technology*, vol. 800-94, no. February, p. 127, 2007. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-94/finalhttp://csrc.nist.gov/publications/drafts/800-94-rev1/draft{_}sp800-94-rev1.pdfhttp://csrc.ncsl.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

[12] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," *Journal of Computer and System Sciences*, vol. 80, no. 5, pp. 973–993, aug 2014. [Online]. Available: http://dx.doi.org/10.1016/j.jcss.2014.02.005https://linkinghub.elsevier.com/retrieve/pii/S0022000014000178

[13] H. Farrell, "Hackers have just dumped a treasure trove of NSA data. Here's what it means." 2017. [Online]. Available: https://www.washingtonpost.com/news/monkey-cage/wp/2017/04/15/shadowy-hackers-have-just-dumped-a-treasure-trove-of-nsa-data-heres-what-it-means/ https://www.washingtonpost.com/news/monkey-cage/wp/2017/04/15/shadowy-hackers-have-just-dumped-a-treasure-trov

[14] G. B. Widagdo and C. Lim, "Analysis of hybrid DDoS defense to mitigate DDoS impact," *Advanced Science Letters*, vol. 23, no. 4, pp. 3633–3639, 2017.

[15] Netscout, "NETSCOUT's 14th Annual Worldwide Infrastructure Security Report," *Netscout*, p. 69, 2019. [Online]. Available: https://www.netscout.com/press-releases/netscout-releases-14th-annual-worldwide-infrastructure---

[16] C. Annual and I. Report, "White paper Cisco public," *White paper Cisco public*, pp. 1–35, 2018. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf

[17] T. Ahmed, B. Oreshkin, and M. Coates, "Machine learning approaches to network anomaly detection," in *2nd Workshop on Tackling Computer Systems Problems with Machine Learning Techniques, SysML 2007, co-located with NSDI 2007*, 2007. [Online]. Available: https://www.usenix.org/legacy/event/sysml07/tech/full{_}papers/ahmed/ahmed{_}html/sysml07CR{_}07.html

[18] Y. Zhou, G. Cheng, S. Jiang, and M. Dai, "An Efficient Intrusion Detection System Based on Feature Selection and Ensemble Classifier," vol. 14, no. 8, pp. 1–12, 2019. [Online]. Available: http://arxiv.org/abs/1904.01352

[19] R. Hananto, C. Lim, and H. P. Ipung, "Detecting network security threats using domain name system and netflow traffic," *ACM International Conference Proceeding Series*, pp. 105–109, 2018.

[20] Canadian Institute for Cybersecurity & University of New Brunswick, "NSL-KDD | Datasets | Research | Canadian Institute for Cybersecurity | UNB," 2009. [Online]. Available: https://www.unb.ca/cic/datasets/nsl.html

[21] W. Liu, X. Liu, X. Di, and H. Qi, "A novel network intrusion detection algorithm based on Fast Fourier Transformation," in *2019 1st International Conference on Industrial Artificial Intelligence (IAI)*. IEEE, jul 2019, pp. 1–6. [Online]. Available: https://ieeexplore.ieee.org/document/8850770/

[22] H. Rafiee and C. Meinel, "Privacy and security in IPv6 networks," 2013, pp. 218–224. [Online]. Available: http://dl.acm.org/citation.cfm?id=1852723{&}dl=ACM{&}

[23] N. Meghanathan, "A tutorial on network security: Attacks and controls," *International Journal on Communications Antenna and Propagation*, vol. 1, no. 1, pp. 103–116, 2011.

[24] A. Russell, "Ideological and Policy Origins of the Internet, 1957-1969," *arXiv preprint cs/0109056*, pp. 1957–1969, 2001.

[25] H. Ren, B. Xu, Y. Wang, C. Yi, C. Huang, X. Kou, T. Xing, M. Yang, J. Tong, and Q. Zhang, "Time-Series Anomaly Detection Service at Microsoft," *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, vol. 3330680, no. c, pp. 3009–3017, jun 2019. [Online]. Available: http://arxiv.org/abs/1906.03821http://dx.doi.org/10.1145/3292500.3330680

[26] CISA, "DoS and DDoS Attacks against Multiple Sectors | CISA." [Online]. Available: https://us-cert.cisa.gov/ncas/current-activity/2020/09/04/dos-and-ddos-attacks-against-multiple-sectors

[27] J. G. Proakis and D. G. Manolakis, *DIGITAL SIGNAL PROCESSING Principles, Algorithms, m l Applications*. PRENTICE-HALL INTERNATIONAL, INC., 2557, vol. 7, no. 2. [Online]. Available: https://engineering.purdue.edu/{~}ee538/DSP{_}Text{_}3rdEdition.pdf

[28] R. F. Fouladi, O. Ermis, and E. Anarim, "Anomaly-Based DDoS Attack Detection by Using Sparse Coding and Frequency Domain," *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC*, vol. 2019-Septe, pp. 1–6, 2019.

[29] T. Dao, A. Gu, M. Eichhorn, A. Rudra, and C. Ré, "Learning fast algorithms for linear transforms using butterfly factorizations," in *36th International Conference on Machine Learning, ICML 2019*, vol. 2019-June, 2019, pp. 2736–2754.

[30] J. W. Cooley and J. W. Tukey, "An Algorithm for the Machine Calculation of Complex Fourier Series," *Mathematics of Computation*, vol. 19, no. 90, p. 297, apr 1965. [Online]. Available: https://www.jstor.org/stable/2003354?origin=crossref

[31] "Confusion Matric(TPR,FPR,FNR,TNR), Precision, Recall, F1-Score | by Namratesh Shrivastav | Data Driven Investor | Medium." [Online].

Available: https://medium.com/datadriveninvestor/confusion-matric-tpr-fpr-fnr-tnr-precision-recall-f1-score-73efa162a25f

[32] B. Xu, H. Shen, Q. Cao, Y. Qiu, and X. Cheng, "Graph Wavelet Neural Network," *7th International Conference on Learning Representations, ICLR 2019*, pp. 1–13, apr 2019. [Online]. Available: http://arxiv.org/abs/1904.07785

[33] W. Cao and W. Zhang, "Machine Learning of Partial Differential Equations from Noise Data," Tech. Rep., sep 2020. [Online]. Available: http://arxiv.org/abs/2010.06507

[34] V. Nair, M. Chatterjee, N. Tavakoli, A. S. Namin, and C. Snoeyink, "Fast Fourier Transformation for Optimizing Convolutional Neural Networks in Object Recognition," 2020. [Online]. Available: http://arxiv.org/abs/2010.04257

[35] R. Gove and L. Deason, "Visualizing Automatically Detected Periodic Network Activity," in *2018 IEEE Symposium on Visualization for Cyber Security (VizSec)*. IEEE, oct 2018, pp. 1–8. [Online]. Available: https://ieeexplore.ieee.org/document/8709177/

[36] S. H. Safavi, M. Khatua, N. M. Cheung, and F. Torkamani-Azar, "On sparse graph fourier transform," 2018. [Online]. Available: https://hal.inria.fr/hal-

[37] Y. Tsuge and H. Tanaka, "Intrusion Detection System Using Discrete Fourier Transform with Window Function," *International Journal of Network Security & Its Applications*, vol. 8, no. 2, pp. 23–34, 2016.

[38] R. Tao, X. Zhao, W. Li, H. C. Li, and Q. Du, "Hyperspectral anomaly detection by fractional fourier entropy," *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 12, no. 12, pp. 4920–4929, 2019.

[39] S.-Y. Ji, B.-K. Jeong, S. Choi, and D. H. Jeong, "A multi-level intrusion detection method for abnormal network behaviors," *Journal of Network and Computer Applications*, vol. 62, pp. 9–17, feb 2016. [Online]. Available: http://dx.doi.org/10.1016/j.jnca.2015.12.004https://linkinghub.elsevier.com/retrieve/pii/S1084804515002970

[40] J. A. Suykens, L. Lukas, and J. Vandewalle, "Sparse approximation using least squares support vector machines," in *Proceedings - IEEE International Symposium on Circuits and Systems*, vol. 2, 2000. [Online]. Available: http://www.esat.kuleuven.be/stadius/ADB/

[41] S. Sapre, P. Ahmadi, and K. Islam, "A Robust Comparison of the KDDCup99 and NSL-KDD IoT Network Intrusion Detection Datasets Through Various Machine Learning Algorithms," 2019. [Online]. Available: http://arxiv.org/abs/1912.13204

[42] B. Ingre and A. Yadav, "Performance analysis of NSL-KDD dataset using ANN," *International Conference on Signal Processing and Communication Engineering Systems - Proceedings of SPACES 2015, in Association with IEEE*, pp. 92–96, 2015.

[43] N. Moustafa, B. Turnbull, and K.-K. R. Choo, "An Ensemble Intrusion Detection Technique Based on Proposed Statistical Flow Features for Protecting Network Traffic of Internet of Things," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4815–4830, jun 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8470090/

[44] M. Idhammad, K. Afdel, and M. Belouch, "Semi-supervised machine learning approach for DDoS detection," *Applied Intelligence*, vol. 48, no. 10, pp. 3193–3208, oct 2018. [Online]. Available: http://link.springer.com/10.1007/s10489-018-1141-2

[45] R. Doshi, N. Apthorpe, and N. Feamster, "Machine learning DDoS detection for consumer internet of things devices," *Proceedings - 2018 IEEE Symposium on Security and Privacy Workshops, SPW 2018*, no. Ml, pp. 29–35, 2018.

[46] R. A. Khamis and A. Matrawy, "Evaluation of Adversarial Training on Different Types of Neural Networks in Deep Learning-based IDSs," 2020.

[47] NumPy.org, "Overview — NumPy v1.19 Manual," pp. 1–1, 2020. [Online]. Available: https://numpy.org/doc/stable/

[48] S. K. Dey and M. M. Rahman, "Flow Based Anomaly Detection in Software Defined Networking: A Deep Learning Approach With Feature Selection Method,"

in *2018 4th International Conference on Electrical Engineering and Information & Communication Technology (iCEEiCT)*. IEEE, sep 2018, pp. 630–635. [Online]. Available: https://ieeexplore.ieee.org/document/8628069/

[49] Scikit-learn, "Recursive feature elimination with cross-validation," 2020. [Online]. Available: https://scikit-learn.org/stable/auto{_}examples/feature{_}selection/plot{_}rfe{_}with{_}cross{_}validation.html?highlight=rfecrossvalidationhttps://scikit-learn.org/stable/auto{_}examples/feature{_}selection/plot{_}rfe{_}with{_}cross{_}validation.html{#}sphx-glr-auto-examples-f

[50] P. Tortoli, "A tracking FFT processor for pulsed Doppler analysis beyond the Nyquist limit." *IEEE transactions on bio-medical engineering*, vol. 36, no. 2, pp. 232–7, feb 1989. [Online]. Available: http://ieeexplore.ieee.org/document/16470/ http://www.ncbi.nlm.nih.gov/pubmed/2917768

[51] "1.1. Python scientific computing ecosystem — Scipy lecture notes." [Online]. Available: http://www.scipy-lectures.org/intro/intro.html{#}why-python

[52] S. Saha, "A Comprehensive Guide to Convolutional Neural Networks — the ELI5 way | by Sumit Saha | Towards Data Science," pp. 1–12, 2018. [Online]. Available: https://towardsdatascience.com/a-comprehensive-guide-to-convolutional-neural-networks-the-eli5-way-3bd2b1164a53

[53] V. Nair, M. Chatterjee, N. Tavakoli, A. S. Namin, and C. Snoeyink, "Fast Fourier Transformation for Optimizing Convolutional Neural Networks in Object Recognition," pp. 1–10, 2020. [Online]. Available: http://arxiv.org/abs/2010.04257