DAFTAR PUSTAKA

[1] D. Septasari, “The Cyber Security and The Challenge of Society 5.0 Era in Indonesia,” *Aisyah J. Informatics Electr. Eng.*, vol. 5, no. 2, pp. 227–233, 2023, doi: 10.30604/jti.v5i2.231.

[2] A. B. Setiawan, “Kajian Strategi Pengamanan Infrastruktur Sumber Daya Informasi Kritis,” *Bul. Pos dan Telekomun.*, vol. 1, no. 1, p. 45, Mar. 2015, doi: 10.17933/bpostel.2015.130104.

[3] A. T. Haryanto, “APJII Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang,” ASOSIASI PENYELENGGARA JASA INTERNET INDONESIA. [Online]. Available: https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang

[4] B. B. Pratama and D. Wijayanti, “Perancangan Model Ekonomi Kreatif 5.0 Berbasis Digital Social Innovation,” *J. Fokus Manaj. Bisnis*, vol. 13, no. 1, pp. 76–90, Apr. 2023, doi: 10.12928/fokus.v13i1.7811.

[5] Id-SIRTII /CC, “Lanskap Keamanan Siber Indonesia,” *Id-SIRTII /CC*, no. 70, pp. 1–107, 2023.

[6] don/HUMAS MENPANRB, “Data BPJS Kesehatan Diduga Bocor, Menteri Tjahjo Dukung Kemkominfo Usut Tuntas,” Menpan.Co.Id. Accessed: Apr. 27, 2025. [Online]. Available: https://www.menpan.go.id/site/berita-terkini/data-bpjs-kesehatan-diduga-bocor-menteri-tjahjo-dukung-kemkominfo-usut-tuntas

[7] CNN Indonesia, “Saksi KPU: Sirekap Terima Serangan dari Dalam dan Luar Negeri,” CNN Indonesia. Accessed: Jul. 13, 2024. [Online]. Available: https://cnnindonesia.com/nasional/20240403122255-617-1082270/saksi-kpu-sirekap-terima-serangan-dari-dalam-dan-luar-negeri

[8] O. Yoachimik, J. Pacheco, and J. Pacheco, “DDoS threat report for 2024 Q2,” The Cloudflare Blog. Accessed: Jul. 13, 2024. [Online]. Available: https://blog.cloudflare.com/ddos-threat-report-for-2024-q2/

[9] O. Yoachimik and J. Pacheco, “4 . 2 Tbps of bad packets and a whole lot more : Cloudflare ’ s Q3 DDoS report Key insights Hyper-volumetric campaign,” 2024.

[10] O. Yoachimik and J. Pacheco, “Serangan DDoS 5 , 6 Tbps yang

memecahkan rekor dan tren DDoS global pada Q4 2024 Sudut pandang unik Cloudflare Wawasan utama DDoS Anatomi serangan DDoS," 2025.

[11] M. T. Intelligence, "Microsoft Digital Defense Report," *Netw. Secur.*, vol. 2024, no. 10, pp. 4–4, 2024, doi: 10.1016/s1353-4858(20)30114-8.

[12] J. Triloka, H. Hartono, and S. Sutedi, "Detection of SQL Injection Attack Using Machine Learning Based On Natural Language Processing," *Int. J. Artif. Intell. Res.*, vol. 6, no. 2, 2022, doi: 10.29099/ijair.v6i2.355.

[13] J. A. Perez-diaz and J. A. Cantoral-ceballos, "Transport and Application Layer DDoS Attacks Detection to IoT," 2022.

[14] BSSN, *Lanskap Keamanan Siber Indonesia*. Jakarta: BSSN, 2023.

[15] S. R. Talpur and T. Kechadi, "A survey on DDoS attacks: Router-based threats and defense mechanism in real-world data centers," *FTC 2016 - Proc. Futur. Technol. Conf.*, no. December, pp. 978–984, 2017, doi: 10.1109/FTC.2016.7821722.

[16] O. Yevsieieva and S. M. Helalat, "Analysis of the impact of the slow HTTP DOS and DDOS attacks on the cloud environment," *2017 4th Int. Sci. Conf. Probl. Infocommunications Sci. Technol. PIC S T 2017 - Proc.*, vol. 2018-Janua, pp. 519–523, 2017, doi: 10.1109/INFOCOMMST.2017.8246453.

[17] M. S. Elsayed, N. A. Le-Khac, S. Dev, and A. D. Jurcut, "DDoSNet: A Deep-Learning Model for Detecting Network Attacks," *Proc. - 21st IEEE Int. Symp. a World Wireless, Mob. Multimed. Networks, WoWMoM 2020*, pp. 391–396, 2020, doi: 10.1109/WoWMoM49955.2020.00072.

[18] H. Beitollahi and G. Deconinck, "Tackling application-layer DDoS Attacks," *Procedia Comput. Sci.*, vol. 10, pp. 432–441, 2012, doi: 10.1016/j.procs.2012.06.056.

[19] M. Asif Khan, M. F. A. Razak, Z. R. B. M. Azmi, A. Firdaus, A. Hafeez Nuhu, and S. Shuja Hussain, "Machine Learning and Deep Learning Approaches for Detecting DDoS Attacks in Cloud Environments," *Fusion Pract. Appl.*, vol. 17, no. 2, pp. 79–97, 2025, doi: 10.54216/FPA.170207.

[20] T. Tan, H. Sama, G. Wijaya, and O. E. Aboagye, "Studi Perbandingan Deteksi Intrusi Jaringan Menggunakan Machine Learning: (Metode SVM

dan ANN) Comparative Study of Network Intrusion Detection Using Machine Learning: (SVM and ANN Method)," *J. Teknol. dan Inf.*, vol. 13, no. September, 2023, doi: 10.34010/jati.v13i2.

[21] G. De Carvalho Bertoli *et al.*, "An End-to-End Framework for Machine Learning-Based Network Intrusion Detection System," *IEEE Access*, vol. 9, pp. 106790–106805, 2021, doi: 10.1109/ACCESS.2021.3101188.

[22] A. Zein *et al.*, "Pengenalan Pembelajaran Mesin dan Deep Learning.," *J. Stud. Alquran dan Tafsir*, vol. 4, no. 1, pp. 29–38, 2023, [Online]. Available: https://jurnal.pranataindonesia.ac.id/index.php/jik/article/download/96/49

[23] A. Devia and B. Soewito, "Analisis Perbandingan Metode Seleksi Fitur untuk Mendeteksi Anomali pada Dataset CIC-IDS-2018," *J. Teknol. Dan Sist. Inf. Bisnis-JTEKSIS*, vol. 5, no. 4, p. 572, 2023, [Online]. Available: http://jurnal.unidha.ac.id/index.php/jteksis

[24] Adrian Pirtama, Yuda Prasetia, Redho Irnindo Saputra, and Eko Arip Winanto, "Improvement Attack Detection on Internet of Thinks Using Principal Component Analysis and Random Forest," *Media J. Gen. Comput. Sci.*, vol. 1, no. 1, pp. 14–19, 2023, doi: 10.62205/mjgcs.v1i1.8.

[25] D. E. S. S. C. Bagyalakshmi, "DDoS Attack Classification on Cloud Environment Using Machine Learning Techniques with Different Feature Selection Methods," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 9, no. 5, pp. 7301–7308, 2020, doi: 10.30534/ijatcse/2020/60952020.

[26] P. R. Kshirsagar, H. Manoharan, H. A. Alterazi, N. Alhebaishi, O. B. J. Rabie, and S. Shitharth, "Construal Attacks on Wireless Data Storage Applications and Unraveling Using Machine Learning Algorithm," *J. Sensors*, vol. 2022, 2022, doi: 10.1155/2022/9386989.

[27] S. Sumathi, R. Rajesh, and S. Lim, "Recurrent and Deep Learning Neural Network Models for DDoS Attack Detection," *J. Sensors*, vol. 2022, 2022, doi: 10.1155/2022/8530312.

[28] J. LI, "Detection of DDoS Attacks based on Dense Neural Networks, Autoencoders and Pearson Correlation Coefficient," *Master Thesis, Comput. Sci. Dept., Dalhousie Univ. Halifax, Nov. Scotia*, no. April, pp. 1–

81, 2020, [Online]. Available: https://dalspace.library.dal.ca/handle/10222/78536

[29] M. Ramzan *et al.*, "Distributed Denial of Service Attack Detection in Network Traffic Using Deep Learning Algorithm," *Sensors (Basel, Switzerland)*, vol. 23, no. 20. 2023. doi: 10.3390/s23208642.

[30] Ahmad Ismail Harry Wicaksono, "Mendeteksi Serangan Distributed Denial of Service (Ddos) Pada Jaringan Komputer," *Thesis (Undergraduate)*, pp. 1–31, 2018, [Online]. Available: https://repository.its.ac.id/id/eprint/53840

[31] H. Chudasama, "Sampling Methods in Research: A Review," *Int. J. Trend Sci. Res. Dev.*, vol. 7, no. 3, pp. 762–768, 2023, [Online]. Available: https://www.researchgate.net/publication/371985656

[32] Y. Li, Y. Yang, P. Song, L. Duan, and R. Ren, "An improved SMOTE algorithm for enhanced imbalanced data classification by expanding sample generation space," pp. 1–21, 2025.

[33] cisco, "What Is Cybersecurity?," cisco. Accessed: Jul. 13, 2024. [Online]. Available: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html?dtid=osscdc000283

[34] Hanafi, *Dasar Cyber Security dan Forensic*. Sleman: deepublish, 2022. [Online]. Available: https://eprints.amikom.ac.id/id/eprint/10688/

[35] Isb. Team, "CIA Triad and New Emerging Technologies: Big Data and IoT," Information Security Buzz. Accessed: Jul. 13, 2024. [Online]. Available: https://informationsecuritybuzz.com/cia-triad-and-new-emerging-technologies-big-data-and-iot/

[36] M. M. Mijwil, I. E. Salem, and M. M. Ismaeel, "The Significance of Machine Learning and Deep Learning Techniques in Cybersecurity: A Comprehensive Review," *Iraqi J. Comput. Sci. Math.*, vol. 4, no. 1, pp. 87–101, 2023, doi: 10.52866/ijcsm.2023.01.01.008.

[37] M. M. Mijwil and E. A. Al-Zubaidi, "Medical image classification for coronavirus disease (covid-19) using convolutional neural networks," *Iraqi J. Sci.*, vol. 62, no. 8, pp. 2740–2747, 2021, doi: 10.24996/ijs.2021.62.8.27.

[38] M. Sarhan, S. Layeghy, N. Moustafa, M. Gallagher, and M. Portmann, "Feature extraction for machine learning-based intrusion detection in IoT

networks," *Digit. Commun. Networks*, vol. 10, no. 1, pp. 205–216, 2024, doi: 10.1016/j.dcan.2022.08.012.

[39] M. A. Teixeira, T. Salman, M. Zolanvari, R. Jain, N. Meskin, and M. Samaka, "SCADA system testbed for cybersecurity research using machine learning approach," *Futur. Internet*, vol. 10, no. 8, 2018, doi: 10.3390/fi10080076.

[40] C. Chairani, W. Widyawan, and S. S. Kusumawardani, "Machine Learning Untuk Estimasi Posisi Objek Berbasis RSS Fingerprint Menggunakan IEEE 802.11g Pada Lantai 3 Gedung JTETI UGM," *J. INFOTEL - Inform. Telekomun. Elektron.*, vol. 7, no. 1, p. 1, 2015, doi: 10.20895/infotel.v7i1.23.

[41] S. S. Nurashila, F. Hamami, and T. F. Kusumasari, "Perbandingan Kinerja Algoritma Recurrent Neural Network (Rnn) Dan Long Short-Term Memory (Lstm): Studi Kasus Prediksi Kemacetan Lalu Lintas Jaringan Pt Xyz," *JIPI (Jurnal Ilm. Penelit. dan Pembelajaran Inform.*, vol. 8, no. 3, pp. 864–877, 2023, doi: 10.29100/jipi.v8i3.3961.

[42] K. Muludi, M. S. Akbar, D. A. Shofiana, and A. Syarif, "Sentiment Analysis Of Energy Independence Tweets Using Simple Recurrent Neural Network," *IJCCS (Indonesian J. Comput. Cybern. Syst.*, vol. 15, no. 4, p. 339, 2021, doi: 10.22146/ijccs.66016.

[43] V. M. Patro and M. R. Patra, "A Novel Approach to Compute Confusion Matrix for Classification of n-Class Attributes with Feature Selection," *Trans. Mach. Learn. Artif. Intell.*, vol. 3, no. 2, 2015.

[44] google, "Welcome to Colab!," google coleb. Accessed: Jul. 13, 2024. [Online]. Available: https://colab.research.google.com/#scrollTo=5fCEDCU_qrC0

[45] phyton, "Python is powerful... and fast; plays well with others; runs everywhere; is friendly & easy to learn; is Open.," phyton. Accessed: Jul. 13, 2024. [Online]. Available: https://www.python.org/about/

[46] S. DEVI, P. Maury, and U. N. Tripathi, "A Novel Method of Using Machine Learning Techniques to Protect Clouds Against Distributed Denial of Service (DDoS) Attacks.," *Babylonian J. Mach. Learn.*, vol.

2024, pp. 133–141, 2024, doi: 10.58496/bjml/2024/013.

[47] R. SaiSindhuTheja and G. K. Shyam, “An efficient metaheuristic algorithm based feature selection and recurrent neural network for DoS attack detection in cloud computing environment,” *Appl. Soft Comput.*, vol. 100, p. 106997, 2021, doi: 10.1016/j.asoc.2020.106997.

[48] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, “Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy,” no. Cic, 2019.

[49] A. S. Raharjo, “Perbandingan Klasifikasi Serangan Jaringan Distributed Denial Of Service (Ddos) Menggunakan Algoritma Decision Tree, K-Nearest Neighbors, Bayesian Network Dan Oner,” 2020. doi: 10.1088/1751-8113/44/8/085201.

[50] S. Susanto, M. A. S. Arifin, and H. O. L. Wijaya, “IoT Botnet Detection Using Autoencoders and Decision Trees,” *J. Sisfokom (Sistem Inf. dan Komputer)*, vol. 12, no. 3, pp. 329–334, 2023, doi: 10.32736/sisfokom.v12i3.1693.

[51] M. K. Anam, S. Defit, Haviluddin, L. Efrizoni, and M. B. Firdaus, “Early Stopping on CNN-LSTM Development to Improve Classification Performance,” *J. Appl. Data Sci.*, vol. 5, no. 3, pp. 1175–1188, 2024, doi: 10.47738/jads.v5i3.312.

[52] A. S. A. Issa and Z. Albayrak, “DDoS Attack Intrusion Detection System Based on Hybridization of CNN and LSTM,” *Acta Polytech. Hungarica*, vol. 20, no. 2, pp. 105–123, 2023, doi: 10.12700/APH.20.2.2023.2.6.

[53] J. Frank, “What is a Timeline? - proposalforNGOs,” no. June, 2014, [Online]. Available: https://proposalsforngos.com/what-is-a-timeline/