DAFTAR PUSTAKA

[1] IBM Security, Cost of a Data Breach Report 2024. IBM Corporation, 2024. [Online]. Available: https://www.ibm.com/security/data-breach

[2] B. Timurlangit, *Perancangan dan Implementasi Private Cloud Infrastructure Menggunakan Proxmox VE pada PT Maro Anugrah Jaya*, MBKM Report, Universitas Multimedia Nusantara, 2025. [Online]. Available: https://kc.umn.ac.id/id/eprint/37899/

[3] Proxmox, "Proxmox Virtual Environment," Proxmox.com. [Online]. Available: https://www.proxmox.com/en/

[4] Fail2Ban, "fail2ban/fail2ban," GitHub. [Online]. Available: https://github.com/fail2ban/fail2ban

[5] Direktorat Keamanan Siber dan Sandi – Kominfo CSIRT, Laporan Tahunan Keamanan Siber 2024. Jakarta: Kementerian Komunikasi dan Informatika, 2024. [Online]. Available: https://csirt.komdigi.go.id/storage/uploads/document_centers/attachments/Laporan%20Tahunan%20Kamsiber%202024.pdf

[6] 4th Platform, WFH: Navigating Cybersecurity in a Remote Work Environment, 07-Aug-2024. [Online]. Available: https://4thplatform.co.uk/2024/08/07/wfh-navigating-cybersecurity-in-a-remote-work-environment/

[7] 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), Shivamogga, India, 2022, pp. 106–111, doi: 10.1109/DISCOVER55800.2022.9974724. [Online]. Available: https://ieeexplore.ieee.org/document/9974724

[8] Detection of the Botnets' Low-Rate DDoS Attacks Based on Self-Similarity, Research Article, 2025. [Online]. Available: https://www.researchgate.net/publication/343366833_Detection_of_the_botnets%27_low-rate_DDoS_attacks_based_on_self-similarity

[9] P. Malhotra, L. Vig, G. Shroff and P. Agarwal, "Long Short-Term Memory Networks for Anomaly Detection in Time Series," TCS Research, 2015. [Online]. Available: https://www.researchgate.net/publication/308947175_Long_Short_Term_Memory_Networks_for_Anomaly_Detection_in_Time_Series

[10] B. Lindemann et al., “A survey on anomaly detection for technical systems using deep neural networks,” Data Mining and Knowledge Discovery, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0166361521001056

[11] A. Singh, “Anomaly Detection for Temporal Data using Long Short-Term Memory (LSTM),” Master’s thesis, KTH Royal Institute of Technology, 2017. [Online]. Available: https://www.diva-portal.org/smash/get/diva2:1149130/FULLTEXT01.pdf

[12] M. D. Hossain, H. Ochiai, F. Doudou and Y. Kadobayashi, "SSH and FTP brute-force Attacks Detection in Computer Networks: LSTM and Machine Learning Approaches," 2020 7th International Conference on Computer and Communication Systems (ICCCS), Kobe, Japan, 2020, pp. 251–256, doi: 10.1109/ICCCS49078.2020.9118459.

[13] B. Gogoi and T. Ahmed, “HTTP Low and Slow DoS Attack Detection using LSTM based deep learning,” in *Proc. 2022 IEEE 19th India Council International Conference (INDICON)*, Kochi, India, Nov. 2022, pp. 1–6, doi: 10.1109/INDICON56171.2022.10039772.

[14] J. Díaz-Verdejo, J. Muñoz-Calle, A. Estepa Alonso, R. Estepa Alonso and G. Madinabeitia, “On the detection capabilities of signature-based intrusion detection systems in the context of web attacks,” *Applied Sciences*, vol. 12, no. 2, art. no. 852, Jan. 2022, doi: 10.3390/app12020852.

[15] M. Catillo, A. Del Vecchio, A. Pecchia, U. Villano and A. Rak, “Transferability of machine learning models learned from public intrusion detection datasets: the CICIDS2017 case study,” Software Quality Journal, vol. 30, pp. 955–981, 2022, doi: 10.1007/s11219-022-09587-0.

[16] A. Sreenivasulu, “Evaluation of cluster-based anomaly detection,” Master’s thesis, School of Informatics, Sweden, 2019. [Online]. Available: https://www.diva-portal.org/smash/get/diva2:1382324/FULLTEXT01.pdf

[17] Proxmox Server Solutions GmbH, Proxmox VE Administration Guide, Proxmox Virtual Environment Documentation. [Online]. Available: https://pve.proxmox.com/pve-docs/pve-admin-guide.html

[18] J. Ylönen and C. Lonvick, *The Secure Shell (SSH) Protocol Architecture*, RFC 4251, Jan. 2006. [Online]. Available: https://www.rfc-editor.org/rfc/rfc4251

[19] SSH Communications Security, “SSH History – Part 1.” [Online]. Available: https://www.ssh.com/about/history/

[20] D. J. Barrett, R. E. Silverman, and R. G. Byrnes, *SSH, the Secure Shell: The Definitive Guide*, 2nd ed. Sebastopol, CA, USA: O'Reilly Media, 2005.

[21] J. Ylönen and C. Lonvick, *The Secure Shell (SSH) Transport Layer Protocol*, RFC 4253, Jan. 2006. [Online]. Available: https://www.rfc-editor.org/rfc/rfc4253

[22] J. Ylönen and C. Lonvick, *The Secure Shell (SSH) Protocol Assigned Numbers*, RFC 4250, Jan. 2006. [Online]. Available: https://www.rfc-editor.org/rfc/rfc4250

[23] J. Ylönen and C. Lonvick, *The Secure Shell (SSH) Connection Protocol*, RFC 4254, Jan. 2006. [Online]. Available: https://www.rfc-editor.org/rfc/rfc4254

[24] SSH Communications Security, "SSH History – Part 3," 2024. [Online]. Available: https://www.ssh.com/about/history/part-3

[25] OpenSSH Project, "OpenSSH Specifications," 2024. [Online]. Available: https://www.openssh.com/specs.html

[26] Z. Zhang and P. Liu, "A hybrid-CPU-FPGA-based solution to the recovery of sha256crypt-hashed passwords," IACR Trans. Cryptogr. Hardw. Embed. Syst., vol. 2020, no. 4, pp. 1–23, 2020, doi: 10.13154/tches.v2020.i4.1-23. [Online]. Available: https://d-nb.info/1221804847/34

[27] V. Kumar and O. P. Sangwan, "Signature based intrusion detection system using SNORT," ResearchGate, 2013. [Online]. Available: https://www.semanticscholar.org/paper/Signature-Based-Intrusion-Detection-System-Using-Kumar-Sangwan/273c6061db3cb2074d3364a295c66251f92ec17e

[28] S. Hochreiter and J. Schmidhuber, "Long Short-Term Memory," Neural Computation, vol. 9, no. 8, pp. 1735–1780, Nov. 1997.

[29] H. Chen, T. Lu, J. Huang, X. He, K. Yu, X. Sun, X. Ma, and Z. Huang, "An improved VMD-LSTM model for time-varying GNSS time series prediction with temporally correlated noise," *Remote Sensing*, vol. 15, no. 14, art. no. 3694, 2023, doi: 10.3390/rs15143694.

[30] F. A. Gers, J. Schmidhuber, and F. Cummins, "Learning to forget: Continual prediction with LSTM," Neural Computation, vol. 12, no. 10, pp. 2451–2471, 2000.

[31] J. Zhu, S. He, P. He, J. Liu, and M. R. Lyu, "Loghub: A large collection of system log datasets for AI-driven log analytics," arXiv:2008.06448 [cs.SE], 2020. doi: 10.48550/arXiv.2008.06448. [Online]. Available: https://arxiv.org/abs/2008.06448

[32] Z. Jiang, J. Liu, J. Huang, Y. Lyu, Y. Su, X. He, P. He, and M. R. Lyu, “A large-scale evaluation for log parsing techniques: How far are we?,” arXiv:2308.10828 [cs.SE], 2023. doi: 10.48550/arXiv.2308.10828. [Online]. Available: https://arxiv.org/abs/2308.10828

[33] GitHub, “GitHub,” 2025. [Online]. Available: https://github.com/

[34] X. Zeng, Y. Hui, J. Shen, A. Pavlo, W. McKinney and H. Zhang, “An empirical evaluation of columnar storage formats,” arXiv:2304.05028 [cs.DB], 2023. [Online]. Available: https://arxiv.org/abs/2304.05028

[35] M. Pourbafrani, S. J. van Zelst, and W. M. P. van der Aalst, “Semi-Automated Time-Granularity Detection for Data-Driven Simulation Using Process Mining and System Dynamics,” in *Conceptual Modeling*, Lecture Notes in Computer Science, vol. 12751, E. Authors, Ed. Cham, Switzerland: Springer, 2020, pp. 77–91, doi: 10.1007/978-3-030-62522-1_6.

[36] J.-K. Lee, S.-J. Kim, C. Y. Park, T. Hong, and H. Chae, “Heavy-tailed distribution of the SSH brute-force attack duration in a multi-user environment,” *J. Korean Phys. Soc.*, vol. 69, no. 2, pp. 253–258, Jul. 2016, doi: 10.3938/jkps.69.253

[37] M. Ester, H.-P. Kriegel, J. Sander, and X. Xu, “A density-based algorithm for discovering clusters in large spatial databases with noise,” in *Proc. 2nd Int. Conf. Knowledge Discovery and Data Mining (KDD ’96)*, Portland, OR, USA, 1996, pp. 226–231.

[38] M. H. Bhuyan, D. K. Bhattacharyya and J. K. Kalita, "Network Anomaly Detection: Methods, Systems and Tools," in *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 303-336, First Quarter 2014, doi: 10.1109/SURV.2013.052213.00046

[39] T. B. Ogunseyi et al., “An explainable LSTM-based intrusion detection system,” Sensors, vol. 25, no. 7, 2025, doi:10.3390/s25072288.

[40] “What is pseudocode?,” *TechTarget*, 27 Jun. 2023. [Online]. Available: https://www.techtarget.com/whatis/definition/pseudocode

[41] “Python Packaging User Guide,” *Python Packaging Authority*, 2025. [Online]. Available: https://packaging.python.org

[42] “Building and Distributing Packages with Setuptools,” setuptools Documentation, 2025. [Online]. Available: https://setuptools.pypa.io/en/latest/setuptools.html

[43] M. Sconzo, “SecRepo.com – Samples of Security Related Data,” *SecRepo*, 2026. [Online]. Available: https://www.secrepo.com/.

[44] “Visual Studio Code,” Microsoft, 2025. [Online]. Available: https://code.visualstudio.com

[45] “Parquet Reader & Viewer Online — Instantly Open & Convert Parquet Files,” ParquetReader.com, 2025. [Online]. Available: https://parquetreader.com/