REFERENCES

[1] R. A. Muzaki, O. C. Briliyant, M. A. Hasditama, and H. Ritchi, "Improving Security of Web-Based Application Using ModSecurity and Reverse Proxy in Web Application Firewall," in *2020 International Workshop on Big Data and Information Security, IWBIS 2020*, Institute of Electrical and Electronics Engineers Inc., Oct. 2020, pp. 85–90. doi: 10.1109/IWBIS50925.2020.9255601.

[2] T. Rahmawati, R. W. Shiddiq, M. Sumpena, S. Setiawan, N. Karna, and S. Hertiana, "Web Application Firewall Using Proxy and Security Information and Event Management for OWASP Cyber Attack Detection," *IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS))*, pp. 280–285, Nov. 2023, doi: 10.1109/IoTaIS60147.2023.10346051.

[3] F. Ahmed, U. Jahangir, H. Rahim, and K. Ali, "Centralized Log Management Using Elasticsearch, Logstash and Kibana," *International Conference on Information Science and Communication Technology*, pp. 1–7, 2020, doi: 10.1109/ICISCT49550.2020.9080053.

[4] A. R. Muhammad, P. Sukarno, and A. A. Wardana, "Integrated Security Information and Event Management (SIEM) with Intrusion Detection System (IDS) for Live Analysis based on Machine Learning," in *Procedia Computer Science*, Elsevier B.V., 2022, pp. 1406–1415. doi: 10.1016/j.procs.2022.12.339.

[5] A. Coscia, V. Dentamaro, S. Galantucci, A. Maci, and G. Pirlo, "Automatic decision tree-based NIDPS ruleset generation for DoS/DDoS attacks," *Journal of Information Security and Applications*, vol. 82, May 2024, doi: 10.1016/j.jisa.2024.103736.

[6] A. S. Alghawli, "Complex methods detect anomalies in real time based on time series analysis," *Alexandria Engineering Journal*, vol. 61, no. 1, pp. 549–561, Jan. 2022, doi: 10.1016/j.aej.2021.06.033.

[7] Z. Noor, S. Hina, F. Hayat, and G. A. Shah, "An intelligent context-aware threat detection and response model for smart cyber-physical systems," *Internet of Things (Netherlands)*, vol. 23, Oct. 2023, doi: 10.1016/j.iot.2023.100843.

[8] F. Ullah, S. Ullah, G. Srivastava, and J. C. W. Lin, "IDS-INT: Intrusion detection system using transformer-based transfer learning for imbalanced network traffic," *Digital Communications and Networks*, vol. 10, no. 1, pp. 190–204, Feb. 2024, doi: 10.1016/j.dcan.2023.03.008.

[9] K. Barik and S. Misra, "IDS-Anta: An open-source code with a defense mechanism to detect adversarial attacks for intrusion detection system," *Software Impacts*, vol. 21, Sep. 2024, doi: 10.1016/j.simpa.2024.100664.

[10] T. Gaber, J. B. Awotunde, M. Torky, S. A. Ajagbe, M. Hammoudeh, and W. Li, "Metaverse-IDS: Deep learning-based intrusion detection system for

Metaverse-IoT networks," *Internet of Things (Netherlands)*, vol. 24, Dec. 2023, doi: 10.1016/j.iot.2023.100977.

[11] A. Adu-Kyere, E. Nigussie, and J. Isoaho, "Analyzing the effectiveness of IDS/IPS in real-time with a custom in-vehicle design," in *Procedia Computer Science*, Elsevier B.V., 2024, pp. 175–183. doi: 10.1016/j.procs.2024.06.013.

[12] T. Bajtoš, P. Sokol, and F. Kurimský, "Processing of IDS alerts in multi-step attacks[Formula presented]," *Software Impacts*, vol. 19, Mar. 2024, doi: 10.1016/j.simpa.2024.100622.

[13] A. Fadhlillah, N. Karna, and A. Irawan, "IDS Performance Analysis using Anomaly-based Detection Method for DOS Attack," in *IoTaIS 2020 - Proceedings: 2020 IEEE International Conference on Internet of Things and Intelligence Systems*, Institute of Electrical and Electronics Engineers Inc., Jan. 2021, pp. 18–22. doi: 10.1109/IoTaIS50849.2021.9359719.

[14] P. TS and P. Shrinivasacharya, "Evaluating neural networks using Bi-Directional LSTM for network IDS (intrusion detection systems) in cyber security," *Global Transitions Proceedings*, vol. 2, no. 2, pp. 448–454, Nov. 2021, doi: 10.1016/j.gltp.2021.08.017.

[15] R. A. Abed, E. K. Hamza, and A. J. Humaidi, "A modified CNN-IDS model for enhancing the efficacy of intrusion detection system," *Measurement: Sensors*, vol. 35, Oct. 2024, doi: 10.1016/j.measen.2024.101299.

[16] A. Bhardwaj, S. Bharany, A. Almogren, A. Ur Rehman, and H. Hamam, "Proactive threat hunting to detect persistent behaviour-based advanced adversaries," *Egyptian Informatics Journal*, vol. 27, Sep. 2024, doi: 10.1016/j.eij.2024.100510.

[17] M. H. Nasir, J. Arshad, and M. M. Khan, "Collaborative device-level botnet detection for internet of things," *Comput Secur*, vol. 129, Jun. 2023, doi: 10.1016/j.cose.2023.103172.

[18] A. Paul, V. Sharma, and O. Olukoya, "SQL injection attack: Detection, prioritization & prevention," *Journal of Information Security and Applications*, vol. 85, Sep. 2024, doi: 10.1016/j.jisa.2024.103871.

[19] M. Abdulridha Hussain *et al.*, "Provably throttling SQLI using an enciphering query and secure matching," *Egyptian Informatics Journal*, vol. 23, no. 4, pp. 145–162, Dec. 2022, doi: 10.1016/j.eij.2022.10.001.

[20] A. C. Rus, M. El-Hajj, and D. K. Sarmah, "NAISS: A reverse proxy approach to mitigate MageCart's e-skimmers in e-commerce," *Comput Secur*, vol. 140, May 2024, doi: 10.1016/j.cose.2024.103797.

[21] L. Shuai and S. Li, "Performance optimization of Snort based on DPDK and Hyperscan," in *Procedia Computer Science*, Elsevier B.V., 2021, pp. 837–843. doi: 10.1016/j.procs.2021.03.007.

[22] I. S. Crespo-Martínez, A. Campazas-Vega, Á. M. Guerrero-Higueras, V. Riego-DelCastillo, C. Álvarez-Aparicio, and C. Fernández-Llamas, "SQL injection attack detection in network flow data," *Comput Secur*, vol. 127, Apr. 2023, doi: 10.1016/j.cose.2023.103093.

[23] D. Bhatnagar, R. J. Subalakshmi, and C. Vanmathi, "Twitter Sentiment Analysis Using Elasticsearch, LOGSTASH and KIBANA," in *International Conference on Emerging Trends in Information Technology and Engineering, ic-ETITE 2020*, Institute of Electrical and Electronics Engineers Inc., Feb. 2020. doi: 10.1109/ic-ETITE47903.2020.351.

[24] S. Adiwal, B. Rajendran, P. S. D., and S. D. Sudarsan, "DNS Intrusion Detection (DID) — A SNORT-based solution to detect DNS Amplification and DNS Tunneling attacks," *Franklin Open*, vol. 2, p. 100010, Mar. 2023, doi: 10.1016/j.fraope.2023.100010.

[25] O. Nyarko-Boateng, I. K. Nti, A. A. Mensah, and E. K. Gyamfi, "Controlling user access with scripting to mitigate cyber-attacks," *Sci Afr*, vol. 26, Dec. 2024, doi: 10.1016/j.sciaf.2024.e02355.

[26] I. T. Wibowo, A. Kurniawan, Noviandri, N. F. Sulaiman, and P. Oktivasari, "Design and Implementation of Cloud Computing Using the NDLC Method Combined with Tunnel Link Split," in *Proceeding - International Conference on Information Technology and Computing 2023, ICITCOM 2023*, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 131–135. doi: 10.1109/ICITCOM60176.2023.10442875.

[27] A. Wiranata, N. Karna, A. Irawan, and A. I. Prakoso, "Implementation and Analysis of Network Security in Raspberry Pi against DOS Attack with HIPS Snort," *International Conference on Computer Science, Information Technology and Engineering (ICCoSITE)*, 2023, doi: https://doi.org/10.1109/ICCoSITE57641.2023.10127741.

[28] X. Huang *et al.*, "Clean: Minimize Switch Queue Length via Transparent ECN-proxy in Campus Networks," in *2021 IEEE/ACM 29th International Symposium on Quality of Service, IWQOS 2021*, Institute of Electrical and Electronics Engineers Inc., Jun. 2021. doi: 10.1109/IWQOS52092.2021.9521295.

[29] D. Arnaldy and T. S. Hati, "Performance Analysis of Reverse Proxy and Web Application Firewall with Telegram Bot as Attack Notification on Web Server," in *2020 3rd International Conference on Computer and Informatics Engineering, IC2IE 2020*, Institute of Electrical and Electronics Engineers Inc., Sep. 2020, pp. 455–459. doi: 10.1109/IC2IE50715.2020.9274592.

[30] M. R. Ahmed and F. M. Ali, "Enhancing Hybrid Intrusion Detection and Prevention System for Flooding Attacks Using Decision Tree," *2019 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE)*, pp. 1–4, 2019, doi: 10.1109/ICCCEEE46830.2019.9071191.

[31] Z. Chiba, N. Abghour, K. Moussaid, O. Lifandali, and R. Kinta, “A Deep Study of Novel Intrusion Detection Systems and Intrusion Prevention Systems for Internet of Things Networks,” in *Procedia Computer Science*, Elsevier B.V., 2022, pp. 94–103. doi: 10.1016/j.procs.2022.10.124.

[32] L. F. Sikos, “Packet analysis for network forensics: A comprehensive survey,” Mar. 01, 2020, *Elsevier Ltd*. doi: 10.1016/j.fsidi.2019.200892.

[33] O. Takaki, N. Hamamoto, A. Takefusa, S. Yokoyama, and K. Aida, “Implementation of Anonymization Algorithms for Log Data Analysis on a Cloud-Based Learning Management System,” in *Procedia Computer Science*, Elsevier B.V., 2023, pp. 3774–3784. doi: 10.1016/j.procs.2023.10.373.

[34] M. Husák, M. Žádník, V. Bartoš, and P. Sokol, “Dataset of intrusion detection alerts from a sharing platform,” *Elsevier*, Nov. 2020, doi: 10.17632/p6tym3fghz.1.

[35] H. Haugerud, H. N. Tran, N. Aitsaadi, and A. Yazidi, “A dynamic and scalable parallel Network Intrusion Detection System using intelligent rule ordering and Network Function Virtualization,” *Future Generation Computer Systems*, vol. 124, pp. 254–267, Nov. 2021, doi: 10.1016/j.future.2021.05.037.

[36] N. Negm *et al.*, “Tasmanian devil optimization with deep autoencoder for intrusion detection in IoT assisted unmanned aerial vehicle networks,” *Ain Shams Engineering Journal*, Nov. 2024, doi: 10.1016/j.asej.2024.102943.

[37] J. Jung, T. Oh, I. Kim, and S. Park, “Open-sourced real-time visualization platform for traffic simulation,” in *Procedia Computer Science*, Elsevier B.V., 2023, pp. 243–250. doi: 10.1016/j.procs.2023.03.033.

[38] V. Devalla, S. Srinivasa Raghavan, S. Maste, J. D. Kotian, and D. Annapurna, “MURLi: A Tool for Detection of Malicious URLs and Injection Attacks,” in *Procedia Computer Science*, Elsevier B.V., 2022, pp. 662–676. doi: 10.1016/j.procs.2022.12.068.

[39] M. A. Lawall, R. A. Shaikh, and S. R. Hassan, “A DDoS Attack Mitigation Framework for IoT Networks using Fog Computing,” in *Procedia Computer Science*, Elsevier B.V., 2021, pp. 13–20. doi: 10.1016/j.procs.2021.02.003.

[40] P. Nespoli, D. Díaz-López, and F. Gómez Mármol, “Cyberprotection in IoT environments: A dynamic rule-based solution to defend smart devices,” *Journal of Information Security and Applications*, vol. 60, Aug. 2021, doi: 10.1016/j.jisa.2021.102878.

[41] S. Alem, D. Espes, L. Nana, E. Martin, and F. De Lamotte, “A novel bi-anomaly-based intrusion detection system approach for industry 4.0,” Aug. 01, 2023, *Elsevier B.V.* doi: 10.1016/j.future.2023.03.024.