REFERENCES

[1] H. Hindy, E. Bayne, M. Bures, R. Atkinson, C. Tachtatzis, and X. Bellekens, "Machine Learning Based IoT Intrusion Detection System: An MQTT Case Study (MQTT-IoT-IDS2020 Dataset)," in *Lecture Notes in Networks and Systems*, 2021, vol. 180. doi: 10.1007/978-3-030-64758-2_6.

[2] A. Lazakidou, K. Siassiakos, and K. Loannou, "Security in Smart Home Environment," in *Wireless technologies for ambient assisted living and healthcare: systems and applications: Systems and applications*, 2010.

[3] S. Fitriani, S. Mandala, and M. A. Murti, "Review of semi-supervised method for Intrusion Detection System," 2017. doi: 10.1109/APMediaCast.2016.7878168.

[4] S. Mandala, K. Jenni, M. A. Ngadi, M. Kamat, and Y. Coulibaly, "Quantifying the severity of blackhole attack in wireless mobile Adhoc networks," in *Communications in Computer and Information Science*, 2014, vol. 467. doi: 10.1007/978-3-662-44966-0_6.

[5] S. Rachmadi, S. Mandala, and D. Oktaria, "Detection of DoS Attack using AdaBoost Algorithm on IoT System," 2021. doi: 10.1109/ICoDSA53588.2021.9617545.

[6] S. Mandala, A. H. Abdullah, A. S. Ismail, H. Haron, M. A. Ngadi, and Y. Coulibaly, "A review of blackhole attack in mobile adhoc network," 2013. doi: 10.1109/ICICI-BME.2013.6698520.

[7] M. Aziz, R. Umar, and F. Ridho, "Implemetasi Jaringan Saraf Tiruan Untuk Mendeteksi Serangan DDoS Pada Forensik Jaringan," 2019.

[8] M. R. Ferdinand, S. Mandala, and D. Oktaria, "Host Vulnerability Analysis Using Supervised Learning Based on Port Response," 2021. doi: 10.1109/ICICyTA53712.2021.9689195.

[9] A. Marzano *et al.*, "The Evolution of Bashlite and Mirai IoT Botnets," in *Proceedings - IEEE Symposium on Computers and Communications*, 2018, vol. 2018-June. doi: 10.1109/ISCC.2018.8538636.

[10] M. Roopak, G. Y. Tian, and J. Chambers, "An Intrusion Detection System Against DDoS Attacks in IoT Networks," 2020. doi: 10.1109/CCWC47524.2020.9031206.

[11] A. Mubarakali, K. Srinivasan, R. Mukhalid, S. C. B. Jaganathan, and N. Marina, "Security challenges in internet of things: Distributed denial of service attack detection using support vector machine-based expert systems," *Computational Intelligence*, vol. 36, no. 4, pp. 1580–1592, Nov. 2020, doi: 10.1111/coin.12293.

[12] L. Huraj, M. Šimon, and T. Horák, "Resistance of IoT sensors against DDOS attack in smart home environment," *Sensors (Switzerland)*, vol. 20, no. 18, pp. 1–23, Sep. 2020, doi: 10.3390/s20185298.

[13] D. Anstee, D. Bussiere, G. Sockrider, and C. Morales, "Worldwide infrastructure security report," Westford, 2017.

[14] F. H. Hsu, Y. L. Hwang, C. Y. Tsai, W. T. Cai, C. H. Lee, and K. W. Chang, "TRAP: A Three-way handshake server for TCP connection establishment," *Applied Sciences (Switzerland)*, vol. 6, no. 11, 2016, doi: 10.3390/app6110358.

[15] L. Tan and N. Wang, "Future Internet: The Internet of Things," in *ICACTE 2010 - 2010 3rd International Conference on Advanced Computer Theory and Engineering, Proceedings*, 2010, vol. 5. doi: 10.1109/ICACTE.2010.5579543.

[16] S. Mandala, S. Novian Anggis, M. Syahrul Mubarok, and Shamila, "Energy efficient IoT thermometer based on fuzzy logic for fever monitoring," 2017. doi: 10.1109/ICoICT.2017.8074640.

[17] S. Haykin, "Neural networks and learning machines, 3/E," Hoboken , 2008.

[18] A. Bode, "K-NEAREST NEIGHBOR DENGAN FEATURE SELECTION MENGGUNAKAN BACKWARD ELIMINATION UNTUK PREDIKSI HARGA KOMODITI KOPI ARABIKA," *ILKOM Jurnal Ilmiah*, vol. 9, no. 2, 2017, doi: 10.33096/ilkom.v9i2.139.188-195.