DAFTAR PUSTAKA

Ahmad, M., Riaz, Q., Zeeshan, M., Tahir, H., Haider, S.A. and Khan, M.S., 2021a. Intrusion detection in internet of things using supervised machine learning based on application and transport layer features using UNSW-NB15 data-set. *Eurasip Journal on Wireless Communications and Networking*, 2021(1). https://doi.org/10.1186/s13638-021-01893-8.

Ahmad, Z., Khan, A.S., Nisar, K., Haider, I., Hassan, R., Haque, M.R., Tarmizi, S. and Rodrigues, J.J.P.C., 2021b. Anomaly detection using deep neural network for iot architecture. *Applied Sciences (Switzerland)*, 11(15). https://doi.org/10.3390/app11157050.

Al-Haija, Q.A. and Zein-Sabatto, S., 2020. An efficient deep-learning-based detection and classification system for cyber-attacks in iot communication networks. *Electronics (Switzerland)*, 9(12), pp.1–26. https://doi.org/10.3390/electronics9122152.

Azizan, A.H., Mostafa, S.A., Mustapha, A., Mohd Foozy, C.F., Abd Wahab, M.H., Mohammed, M.A. and Khalaf, B.A., 2021. A machine learning approach for improving the performance of network intrusion detection systems. *Annals of Emerging Technologies in Computing*, 5(Special issue 5), pp.201–208. https://doi.org/10.33166/AETiC.2021.05.025.

Babovic, Z.B., Protic, J. and Milutinovic, V., 2016. Web Performance Evaluation for Internet of Things Applications. *IEEE Access*, 4, pp.6974–6992. https://doi.org/10.1109/ACCESS.2016.2615181.

Bagaa, M., Taleb, T., Bernabe, J.B. and Skarmeta, A., 2020. A Machine Learning Security Framework for Iot Systems. *IEEE Access*, 8, pp.114066–114077. https://doi.org/10.1109/ACCESS.2020.2996214.

Dr. S. Smys, Dr. Abul Basar and Dr. Haoxiang Wang, 2020. Hybrid Intrusion Detection System for Internet of Things (IoT). *Journal of ISMAC*, 2(4), pp.190–199. https://doi.org/10.36548/jismac.2020.4.002.

Ennaji, S., Akkad, N. El and Haddouch, K., 2021. A Powerful Ensemble Learning Approach for Improving Network Intrusion Detection System (NIDS). In: *5th International Conference on Intelligent Computing in Data Sciences, ICDS 2021*. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICDS53782.2021.9626727.

Gyamfi, E. and Jurcut, A., 2022. *Intrusion Detection in Internet of Things Systems: A Review on Design Approaches Leveraging Multi-Access Edge Computing, Machine Learning, and Datasets*. *Sensors*, https://doi.org/10.3390/s22103744.

Hoelz, B.W.P., Ralha, C.G., Geeverghese, R. and Junior, H.C., 2008. MADIK: A Collaborative Multi-agent ToolKit to Computer Forensics. In: R. Meersman, Z. Tari and P. Herrero, eds. *On the Move to Meaningful Internet Systems: OTM 2008 Workshops*. Berlin, Heidelberg: Springer Berlin Heidelberg. pp.20–21.

Injadat, M., Moubayed, A., Nassif, A.B. and Shami, A., 2021. Multi-Stage Optimized Machine Learning Framework for Network Intrusion Detection. *IEEE Transactions on Network and Service Management*, 18(2), pp.1803–1816. https://doi.org/10.1109/TNSM.2020.3014929.

Keserwani, P.K., Govil, M.C., Pilli, E.S. and Govil, P., 2021. A smart anomaly-based intrusion detection system for the Internet of Things (IoT) network using GWO–PSO–RF model. *Journal of Reliable Intelligent Environments*, 7(1), pp.3–21. https://doi.org/10.1007/s40860-020-00126-x.

Kumar, S., Tiwari, P. and Zymbler, M., 2019. Internet of Things is a revolutionary approach for future technology enhancement: a review. *Journal of Big Data*, 6(1). https://doi.org/10.1186/s40537-019-0268-2.

Laghrissi, F.E., Douzi, S., Douzi, K. and Hssina, B., 2021. Intrusion detection systems using long short-term memory (LSTM). *Journal of Big Data*, 8(1). https://doi.org/10.1186/s40537-021-00448-4.

Mahesh, B., 2020. Machine Learning Algorithms - A Review. *International Journal of Science and Research (IJSR)*, 9(1), pp.381–386. https://doi.org/10.21275/art20203995.

Manimurugan, S., 2021. IoT-Fog-Cloud model for anomaly detection using improved Naïve Bayes and principal component analysis. *Journal of Ambient Intelligence and Humanized Computing*. https://doi.org/10.1007/s12652-020-02723-3.

Mohammed, M., Khan, M.B. and Bashie, E.B.M., 2016. *Machine learning: Algorithms and applications*. *Machine Learning: Algorithms and Applications*. CRC Press. https://doi.org/10.1201/9781315371658.

Mukherjee, S. and Haque, S., 2018. *Review Paper on Digital Forensics Practices: A Road Map for Building Digital Forensics Capability*.

Naqa, I. El and Murphy, M.J., 2015. Machine Learning in Radiation Oncology. *Machine Learning in Radiation Oncology*, pp.3–11. https://doi.org/10.1007/978-3-319-18305-3.

Pedregosa FABIANPEDREGOSA, F., Michel, V., Grisel OLIVIERGRISEL, O., Blondel, M., Prettenhofer, P., Weiss, R., Vanderplas, J., Cournapeau, D., Pedregosa, F., Varoquaux, G., Gramfort, A., Thirion, B., Grisel, O., Dubourg, V., Passos, A., Brucher, M., Perrot andÉdouardand, M., Duchesnay, andÉdouard and Duchesnay EDOUARDDUCHESNAY, Fré., 2011. *Scikit-learn: Machine Learning in Python Gaël Varoquaux Bertrand Thirion Vincent Dubourg Alexandre Passos PEDREGOSA, VAROQUAUX, GRAMFORT ET AL. Matthieu Perrot*. [online] *Journal of Machine Learning Research*, Available at: <http://scikit-learn.sourceforge.net.>.

Rashid, M.M., Kamruzzaman, J., Hassan, M.M., Imam, T. and Gordon, S., 2020. Cyberattacks detection in iot-based smart city applications using machine learning techniques. *International Journal of Environmental Research and Public Health*, 17(24), pp.1–21. https://doi.org/10.3390/ijerph17249347.

Saharkhizan, M., Azmoodeh, A., Dehghantanha, A., Choo, K.K.R. and Parizi, R.M., 2020. An Ensemble of Deep Recurrent Neural Networks for Detecting IoT

Cyber Attacks Using Network Traffic. *IEEE Internet of Things Journal*, 7(9), pp.8852–8859. https://doi.org/10.1109/JIOT.2020.2996425.

Sarker, I.H., Alqahtani, H., Alsolami, F., Khan, A.I., Abushark, Y.B. and Siddiqui, M.K., 2020. Context pre-modeling: an empirical analysis for classification based user-centric context-aware predictive modeling. *Journal of Big Data*, 7(1). https://doi.org/10.1186/s40537-020-00328-3.

Singh, N.B., Singh, M.M., Sarkar, A. and Mandal, J.K., 2021. A novel wide & deep transfer learning stacked GRU framework for network intrusion detection. *Journal of Information Security and Applications*, 61. https://doi.org/10.1016/j.jisa.2021.102899.

Thamilarasu, G. and Chawla, S., 2019. Towards deep-learning-driven intrusion detection for the internet of things. *Sensors (Switzerland)*, 19(9). https://doi.org/10.3390/s19091977.