DAFTAR PUSTAKA

Ahmad, I., Basheri, M., Iqbal, M. J., & Rahim, A. (2018). Performance Comparison of Support Vector Machine, Random Forest, and Extreme Learning Machine for Intrusion Detection. *IEEE Access*, *6*(c), 33789–33795. https://doi.org/10.1109/ACCESS.2018.2841987

Anuar, N. B., Papadaki, M., Furnell, S., & Clarke, N. (2013). Incident prioritisation using analytic hierarchy process (AHP): Risk Index Model (RIM). *Security and Communication Networks*, *6*(9), 1087–1116. https://doi.org/10.1002/sec.673

Anwar, F., Khan, B. U. I., Olanrewaju, R. F., Pampori, B. R., & Mir, R. N. (2020). A comprehensive insight into game theory in relevance to cyber security. *Indonesian Journal of Electrical Engineering and Informatics*, *8*(1), 189–203. https://doi.org/10.11591/ijeei.v8i1.1810

Bamhdi, A. M., Abrar, I., & Masoodi, F. (2021). *An ensemble based approach for effective intrusion detection using majority voting*. *19*(2), 664–671. https://doi.org/10.12928/TELKOMNIKA.v19i2.18325

Bu, S. J., & Cho, S. B. (2020). A convolutional neural-based learning classifier system for detecting database intrusion via insider attack. *Information Sciences*, *512*, 123–136. https://doi.org/10.1016/j.ins.2019.09.055

Budiman, S., Sunyoto, A., & Nasiri, A. (2021). Analisa Performa Penggunaan Feature Selection untuk Mendeteksi Intrusion Detection Systems dengan Algoritma

Random Forest Classifier. *Sistemasi*, *10*(3), 753. https://doi.org/10.32520/stmsi.v10i3.1550

Chen, C. M., Chen, Y. L., & Lin, H. C. (2010). An efficient network intrusion detection. *Computer Communications*, *33*(4), 477–484. https://doi.org/10.1016/j.comcom.2009.10.010

Gabet, J., & Yoshida, N. (2020). Static Race Detection and Mutex Safety and Liveness for Go Programs (extended version). *ArXiv*.

Hamid, T. M. T. A., Sallehuddin, R., Yunos, Z. M., & Ali, A. (2021). Ensemble Based Filter Feature Selection with Harmonize Particle Swarm Optimization and Support Vector Machine for Optimal Cancer Classification. *Machine Learning with Applications*, *5*(December 2020), 100054. https://doi.org/10.1016/j.mlwa.2021.100054

Hamid, Y., Balasaraswathi, V. R., Journaux, L., & Sugumaran, M. (2018). Benchmark Datasets for Network Intrusion Detection: A Review. *International Journal of Network Security*, *20*(4), 7. https://doi.org/10.6633/IJNS.2018xx.20(x).xx

Hsu, C. M., Azhari, M. Z., Hsieh, H. Y., Prakosa, S. W., & Leu, J. S. (2020). Robust Network Intrusion Detection Scheme Using Long-Short Term Memory Based Convolutional Neural Networks. *Mobile Networks and Applications*. https://doi.org/10.1007/s11036-020-01623-2

Hu, W., Member, S., Hu, W., & Maybank, S. (2008). AdaBoost-Based Algorithm for

Network. *Ieee Transactions on Systems, Man, and Cybernetics*, *38*(2), 577–583.

Jasim, Y. A. (2018). Improving Intrusion Detection Systems Using Artificial Neural Networks. *ADCAIJ: Advances in Distributed Computing and Articial Intelligence Journal*, *7*(2), 49–65. https://doi.org/http://dx.doi.org/10.14201/ADCAIJ2018714965

Kamarudin, M. H., Maple, C., & Watson, T. (2019). Hybrid feature selection technique for intrusion detection system. *International Journal of High Performance Computing and Networking*, *13*(2), 232. https://doi.org/10.1504/ijhpcn.2019.097503

Kasongo, S. M., & Sun, Y. (2020). Performance Analysis of Intrusion Detection Systems Using a Feature Selection Method on the UNSW-NB15 Dataset. *Journal of Big Data*, *7*(1). https://doi.org/10.1186/s40537-020-00379-6

Kavitha, G., & Elango, N. M. (2020). An approach to feature selection in intrusion detection systems using machine learning algorithms. *International Journal of E-Collaboration*, *16*(4), 48–58. https://doi.org/10.4018/IJeC.2020100104

Kim, K., Erza, M., Harry, A., & Tanuwidjaja, C. (2018). *Network Intrusion Detection using Deep Learning A Feature Learning Approach*.

Kozhevnikov, V. A., Sabinin, O. Y., & Shats, J. E. (2017). LIBRARY DEVELOPMENT FOR CREATING BOTS ON SLACK, TELEGRAM AND FACEBOOK MESSENGERS. *International Scientific Journal Theoretical &*

Applied Science P-ISSN:, *50*(06), 59–62. https://doi.org/10.15863/TAS

Harjoseputro, Y., Kristanto, A. A., & Samodra, J. E. (2020). Implementasi Golang dan New Simple Queue pada Sistem Sandbox Pihak Ketiga Berbasis REST API. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *4*(4), 745–750.

Li, W., & Li, Q. X. (2010). Using naive Bayes with AdaBoost to enhance network anomaly intrusion detection. *Proceedings - 3rd International Conference on Intelligent Networks and Intelligent Systems, ICINIS 2010*, 486–489. https://doi.org/10.1109/ICINIS.2010.133

Liu, G., & Zhang, J. (2020). CNID: Research of Network Intrusion Detection Based on Convolutional Neural Network. *Discrete Dynamics in Nature and Society*, *2020*. https://doi.org/10.1155/2020/4705982

Liu, Z., Chang, B., & Cheng, F. (2021). An interactive filter-wrapper multi-objective evolutionary algorithm for feature selection. *Swarm and Evolutionary Computation*, *65*(August 2020), 100925. https://doi.org/10.1016/j.swevo.2021.100925

Majidpour, J., & Hasanzadeh, H. (2020). Application of deep learning to enhance the accuracy of intrusion detection in modern computer networks. *Bulletin of Electrical Engineering and Informatics*, *9*(3), 1137–1148. https://doi.org/10.11591/eei.v9i3.1724

Meng, Y., & Kwok, L. F. (2014). Adaptive blacklist-based packet filter with a statistic-

based approach in network intrusion detection. *Journal of Network and Computer Applications*, *39*(1), 83–92. https://doi.org/10.1016/j.jnca.2013.05.009

Min, E., Long, J., Liu, Q., Cui, J., & Chen, W. (2018). TR-IDS: Anomaly-Based Intrusion Detection through Text-Convolutional Neural Network and Random Forest. *Security and Communication Networks*, *2018*. https://doi.org/10.1155/2018/4943509

Mir, S. Q., Mir, I. A., & Beiigh, B. M. (2018). Investigating the denial of service attack : A major threat to internet and the security of information. *JK Research Journal in Mathematics and Computer Sciences Investigating*, *1*(1), 121–131.

Nguyen, M. T., & Kim, K. (2020). Genetic convolutional neural network for intrusion detection systems. *Future Generation Computer Systems*, *113*, 418–427. https://doi.org/10.1016/j.future.2020.07.042

Noel, S., & Jajodia, S. (2008). Optimal IDS sensor placement and alert prioritization using attack graphs. *Journal of Network and Systems Management*, *16*(3), 259–275. https://doi.org/10.1007/s10922-008-9109-x

Putri, N. L., Nugroho, R. A., & Herteno, R. (2021). Intrusion Detection System Berbasis Seleksi Fitur Dengan Kombinasi Filter Information Gain Ratio Dan Correlation. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *8*(3), 457. https://doi.org/10.25126/jtiik.0813154

Rustam, F., Reshi, A. A., Aljedaani, W., Alhossan, A., Ishaq, A., Shafi, S., Lee, E.,

Alrabiah, Z., Alsuwailem, H., Ahmad, A., & Rupapara, V. (2022). Vector mosquito image classification using novel RIFS feature selection and machine learning models for disease epidemiology. *Saudi Journal of Biological Sciences*, *29*(1), 583–594. https://doi.org/10.1016/j.sjbs.2021.09.021

Sohal, A. S., Sandhu, R., Sood, S. K., & Chang, V. (2018). A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments. *Computers and Security*, *74*, 340–354. https://doi.org/10.1016/j.cose.2017.08.016

Sun, P., Liu, P., Li, Q., Liu, C., Lu, X., Hao, R., & Chen, J. (2020). DL-IDS: Extracting features using CNN-LSTM hybrid network for intrusion detection system. *Security and Communication Networks*, *2020*. https://doi.org/10.1155/2020/8890306

Syarif, I., Zaluska, E., Prugel-Bennett, A., & Wills, G. (2012). Application of bagging, boosting and stacking to intrusion detection. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *7376 LNAI*, 593–602. https://doi.org/10.1007/978-3-642-31537-4_46

Thabit H Thabit and Yaser A Jasim. (2017). Applying IT in Accounting Environment and Computer Science Studies. In *Environment and Computer Science Studies, LAP-Lambert Academic Publisher, Germany*. Scholars' Press.

Wang, S., Li, C., & Lim, A. (2021). A Model for Non-Stationary Time Series and its

Applications in Filtering and Anomaly Detection. *IEEE Transactions on Instrumentation and Measurement*, *70*. https://doi.org/10.1109/TIM.2021.3059321

Wu, K., Chen, Z., & Li, W. (2018). A Novel Intrusion Detection Model for a Massive Network Using Convolutional Neural Networks. *IEEE Access*, *6*(October 2017), 50850–50859. https://doi.org/10.1109/ACCESS.2018.2868993

Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & de Alvarenga, S. C. (2017). A survey of intrusion detection in Internet of Things. *Journal of Network and Computer Applications*, *84*(February), 25–37. https://doi.org/10.1016/j.jnca.2017.02.009

Zhang, J., Ling, Y., Fu, X., Yang, X., Xiong, G., & Zhang, R. (2020). Model of the intrusion detection system based on the integration of spatial-temporal features. *Computers and Security*, *89*, 101681. https://doi.org/10.1016/j.cose.2019.101681

Zomlot, L., Sundaramurthy, S. C., Luo, K., Ou, X., & Rajagopalan, S. R. (2011). Prioritizing intrusion analysis using dempster-shafer theory. *Proceedings of the ACM Conference on Computer and Communications Security*, *October*, 59–69. https://doi.org/10.1145/2046684.2046694