DAFTAR PUSTAKA

Adler, A., Podio, F. L., Herr, F., Cao, K., Tian, J., Zhang, Y., … Zektser, G. (2009). Cross-Validation. *Encyclopedia of Biometrics*, 206–206. https://doi.org/10.1007/978-0-387-73003-5_615

Afaq, M., Rehman, S., & Song, W.-C. (2015). Large Flows Detection, Marking, and Mitigation based on sFlow Standard in SDN. *Journal of Korea Multimedia Society*, *18*(2), 189–198. https://doi.org/10.9717/kmms.2015.18.2.189

Biau, G. (2012). Analysis of a Random Forests Model. *Journal OfMachine Learning Research 13*, *49*(5), 373–381. https://doi.org/10.5603/AIT.a2017.0074

Breiman, L. E. O. (2001). Random Forests. *Kluwer Academic Publishers*, *45*, 5–32. https://doi.org/10.1023/A:1010933404324

Chris, N. (2015). SDN Implementation-Test on Mikrotik. *Citraweb Nusa Infomedia*.

CIC@unb.ca. (2018). A Realistic Cyber Defense Dataset (CSE-CIC-IDS2018). Retrieved from https://registry.opendata.aws/cse-cic-ids2018

Delamer, A. (2002). Intrusion Detection with Data Mining. *Donau-Universität Krems*.

Foundation, O. N. (2012). Software-Defined Networking: The New Norm for Networks [white paper]. *ONF White Paper*, 1–12. https://doi.org/citeulike-article-id:12475417

Hasan, M. A. M., Nasser, M., Ahmad, S., & Molla, K. I. (2016). Feature Selection for Intrusion Detection Using Random Forest. *Journal of Information Security*, *07*(03), 129–140. https://doi.org/10.4236/jis.2016.73009

Hermawan, R. (2015). Analisis Konsep Dan Cara Kerja Serangan Komputer Distributed Denial of Service (DDOS). *Faktor Exacta*, *5*(1), 1–14.

Hidayat, M. H. (2017). *Implementasi Dan Analisis Kinerja Arsitektur Software-Defined Network Berbasis Opendaylight Controller*. Universitas Gadjah Mada.

Hurwitz, J., & Kirsch, D. (2018). *Machine Learning For Dummies®, IBM Limited Edition Published*. New Jersey: John Wiley & Sons, Inc.

Kartadie, R., Utami, E., & Pramono, E. (2014). PROTOTIPE INFRASTRUKTUR SOFTWARE-DEFINED NETWORK DENGAN PROTOKOL OPENFLOW MENGGUNAKAN UBUNTU SEBAGAI KONTROLER. *Jurnal Dasi*, *15*(1), 24–32.

Kiana, Y., & Saelan, D. P. (2012). Kajian Mengenai Standar Deviasi Hasil Uji Tekan Beton, (November), 49–56.

Lawal, B. H., & At, N. (2018). Improving Software Defined Network Security via sFLow and IPSec Protocol. *Anadolu University Journal of Science and Technology-A Applied Sciences and Engineering*, *19*(3), 555–564. https://doi.org/10.18038/aubtda.421939

Li, B., Gunes, M. H., Bebis, G., & Springer, J. (2013). A Supervised Machine Learning Approach to Classify Host Roles On Line Using sFlow. *HPPN'13 New Year City*, *1*, 53–60. https://doi.org/10.1145/2465839.2465847

Marlita, O. A., Kurniati, A. P., & Informatika, F. (2015). Anomaly Detection pada Intrusion Detection System (IDS) Menggunakan Metode Bayesian Network. *Jurnal Penelitian Dan Pengembangan Telekomunikasi*, *17*(1), 53–61.

Mawardana, R. A. (2018). *Perbandingan Akurasi Naive Bayes, Decision Tree Dan Random Forest Classifier Dalam Memprediksi Hasil Pertandingan League Of Legends Berbasis Spesifikasi Karakter*. *Universitas Gadjah Mada*.

Mckeown, N., Anderson, T., Peterson, L., Rexford, J., Shenker, S., & Louis, S. (2008). OpenFlow: Enabling Innovation in Campus Networks. *ACM SIGCOMM Computer Communication Review*, *38*(2), 69–74. https://doi.org/10.1145/1355734.1355746

Mongkareng, D., Setiawan, N. A., & Permanasari, A. E. (2017). Implementasi Data

Mining dengan Seleksi Fitur untuk Klasifikasi Serangan pada Intrusion Detection System (IDS). *Citee*, 314–321.

Norena, S. (2018). Python Model Tuning Methods Using Cross Validation and Grid Search. Retrieved May 19, 2019, from https://medium.com/@sebastiannorena/some-model-tuning-methods-bfef3e6544f0

Nugraha, M., Paramita, I., Musa, A., Choi, D., & Cho, B. (2014). Utilizing OpenFlow and sFlow to Detect and Mitigate SYN Flooding Attack. *Journal of Korea Multimedia Society*, *17*(8), 988–994. https://doi.org/10.9717/kmms.2014.17.8.988

Nurhasanah. (2008). Metode pencegahan serangan Denial of Services. Palembang: UNIVERSITAS SRIWIJAYA.

Onosproject. (2017). What is ONOS? Retrieved March 1, 2019, from https://wiki.onosproject.org/

Patrikakis, C., Masikos, M., & Zouraraki, O. (2004). Distributed Denial of Service Attacks. *The Internet Protocol Journal, Cisco Systems*, *7*(4), 13–35. Retrieved from www.cisco.com/ipj

Setiawan, H. H. (2018). *Klasifikasi Jenis Buah Pisang Dengan Image Processing Menggunakan Methode Backpropagation*.

SFlow-RT. (2019). sFlow-RT. Retrieved March 1, 2019, from https://sflow-rt.com

Sharafaldin, I., Habibi Lashkari, A., & Ghorbani, A. A. (2018). Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. *ICISSP 2018 - 4th International Conference on Information Systems Security and Privacy Sis*, 108–116. https://doi.org/10.5220/0006639801080116

Sugiyono. (2007). *Statistika untuk Penelitian* (Vol. 2018-July). Alfabeta Bandung. https://doi.org/10.1109/EMBC.2018.8512206

Ummah, I., & Abdillah, D. (2016). Perancangan Simulasi Jaringan Virtual Berbasis Software-Define Networking. *Indonesian Journal on Computing (Indo-JC),*

1(1), 95–106. https://doi.org/10.21108/indojc.2016.1.1.20

Vishnoi, A., & Kumbhare, A. (2013). Open Flow 1.3.1 Support: Controller View. *IBM*. Retrieved from https://wiki.opendaylight.org/images/d/dc/Openflow1.3_Support_for_Opendaylight.pdf

Walpole, R. E., Myers, R. H., Myers, S. L., & Ye, K. (2012). *Probability & statistics for engineers & scientists*. *Education* (Vol. 6). https://doi.org/10.2307/2288012

Wihardi, Y. (2013). K-Folds Cross Validation. Retrieved May 19, 2019, from http://blog.yayaw.web.id/riset/k-folds-cross-validation

Yasin, A., Utami, E., & Pramono, E. (2016). PENGUJIAN SERANGAN DISTRIBUTED DENIAL OF SERVICE (DDOS) DI JARINGAN SOFTWARE-DEFINED PADA GNS3. *Jurnal Teknologi Informasi*, *XI*(32), 2–8.

Zheng, A. (2015). *Evaluating Machine Learning Algorithms: A Beginner's Guide to Key Concepts and Pitfalls*.