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.

Aljawarneh, S., Aldwairi, M., & Yassein, M. B. (2018). Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. *Journal of Computational Science*, *25*, 152–160.

Boyer, S. (2004). *SCADA - Supervisory Control and Data Acquisition. ISA 3rd Edition* (p. 204).

Celiktas, B., Serkan Tok, M., & Unlu, N. (2018). Man in the Middle (MITM) Attack Detection Tool Design. *International Journal of Engineering Sciences & Research Technology*, *7*(8), 90–99.

Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., & Faruki, P. (2019). Network Intrusion Detection for IoT Security Based on Learning Techniques. *IEEE Communications Surveys and Tutorials*, *21*(3), 2671–2701.

Chambali, M., & Muhammad, A. W. (2018). *Klasifikasi Paket Jaringan Berbasis Analisis Statistik dan Neural Network*. *03*(1), 67–70.

Chen, B., Pattanaik, N., Goulart, A., Butler-Purry, K. L., & Kundur, D. (2015). Implementing attacks for modbus/TCP protocol in a real-time cyber physical system test bed. *Proceedings - CQR 2015: 2015 IEEE International Workshop Technical Committee on Communications Quality and Reliability*.

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers and Security*, *56*, 1–27.

Colbert, E. J. M., Sullivan, D. T., & Kott, A. (2016). *Cyber-Physical War Gaming SCADA and Industrial Control Systems*.

Conti, M., Dragoni, N., & Lesyk, V. (2016). A Survey of Man in the Middle Attacks. *IEEE Communications Surveys and Tutorials*, *18*(3), 2027–2051.

Deng, X., Liu, Q., Deng, Y., & Mahadevan, S. (2016). An improved method to construct basic probability assignment based on the confusion matrix for classification problem. *Information Sciences*, *340–341*, 250–261.

Eigner, O., Kreimel, P., & Tavolato, P. (2017). Detection of man-in-the-middle attacks on industrial control networks. *Proceedings - 2016 International Conference on Software Security and Assurance, ICSSA 2016*, 64–69.

Hodo, E., Grebeniuk, S., Ruotsalainen, H., & Tavolato, P. (2017). Anomaly detection for simulated IEC-60870-5-104 traffic. *ACM International Conference Proceeding Series*, *Part F1305*.

Kamesh, & Sakthi Priya, N. (2012). A survey of cyber crimes Yanping. *Security and Communication Networks*, *5*(June), 422–437.

Kaja, N., Shaout, A., & Ma, D. (2019). An intelligent intrusion detection system. *Applied Intelligence*, *49*(9), 3235–3247.

Kunang, Y. N., Nurmaini, S., Stiawan, D., Zarkasi, A., & Jasmir, F. (2019). Automatic Features Extraction Using Autoencoder in Intrusion Detection System. *Proceedings of 2018 International Conference on Electrical Engineering and Computer Science, ICECOS 2018*, *1*, 219–224.

Kurnaz, S., & Obaid, I. A. (2019). *Support Vector Machine (SVM) Based on Wavelet Transform (WT) for Intrusion Detection System (IDS). 8 pp21*(2), 13–19.

Leahy, K., Lily Hu, R., C. Konstantakopoulos, I., J. Spanos, C., M. Agogino, A., & T. J. O'Sullivan, D. (2020). Diagnosing and PredictingWind Turbine Faults from SCADA Data Using Support Vector Machines. *International Journal of Prognostics and Health Management*, *9*(1), 0–11.

Lin, C. Y., & Nadjm-Tehrani, S. (2018). Understanding IEC-60870-5-104 traffic patterns in SCADA networks. *CPSS 2018 - Proceedings of the 4th ACM Workshop on Cyber-Physical System Security, Co-Located with ASIA CCS 2018*, 51–60.

Matousek, P., Ryšavý, O., & Gregr, M. (2019). *Increasing Visibility of IEC 104 Communication in the Smart Grid*. *October*.

Maynard, P., McLaughlin, K., & Sezer, S. (2018). *An Open Framework for Deploying Experimental SCADA Testbed Networks*. *2016*, 92–101.

Maynard, P., & Mclaughlin, K. (2014). *Towards Understanding Man-In-The-Middle Attacks on IEC 60870-5-104 SCADA Networks*. 30–42.

Prasetyo, A., Affandi, L., & Arpandi, D. (2018). Implementasi Metode Naive Bayes Untuk Intrusion Detection System (Ids). *Jurnal Informatika Polinema*, *4*(4), 280.

Qassim, Q. S., Jamil, N., Daud, M., Ja'affar, N., Yussof, S., Ismail, R., & Kamarulzaman, W. A. W. (2018). Simulating command injection attacks on IEC 60870-5-104 protocol in SCADA system. *International Journal of Engineering and Technology(UAE)*, *7*(2.14 Special Issue 14), 153–159.

Radoglou-Grammatikis, P., Sarigiannidis, P., Giannoulakis, I., Kafetzakis, E., & Panaousis, E. (2019). Attacking IEC-60870-5-104 SCADA Systems. *Proceedings - 2019 IEEE World Congress on Services, SERVICES 2019*, *2642-939X*, 41–46.

Riadi, I., Umar, R., & Aini, F. D. (2019). Analisis Perbandingan Detection Traffic Anomaly Dengan Metode Naive Bayes Dan Support Vector Machine (Svm). *ILKOM Jurnal Ilmiah*, *11*(1), 17–24.

Saputra, E., Khaira, U., & Abidin, Z. (2021). Implementasi Algoritme Support Vector Machines untuk Klasifikasi Area Terbakar di Lahan Gambut (Implementation of Support Vector Machines Algorithm to Classify Burn Area of Peat). *Jurnal Nasional Teknik Elektro Dan Teknologi Informasi*, *10*(1), 19–24.

Sebbar, A., Zkik, K., Baddi, Y., Boulmalf, M., & Kettani, M. D. E. C. El. (2020). MitM detection and defense mechanism CBNA-RF based on machine learning for large-scale SDN context. *Journal of Ambient Intelligence and Humanized Computing*, *11*(12), 5875–5894.

Teixeira, M. A., Salman, T., Zolanvari, M., Jain, R., Meskin, N., & Samaka, M. (2018). SCADA system testbed for cybersecurity research using machine learning approach. *Future Internet*, *10*(8).

Yang, Y., McLaughlin, K., Littler, T., Sezer, S., & Wang, H. F. (2013). Rule-based Intrusion Detection System for SCADA networks. *IET Conference Publications*, *2013*(623 CP), 2–5.

Yang, Y., McLaughlin, K., Littler, T., Sezer, S., Pranggono, B., & Wang, H. F. (2013). Intrusion Detection System for IEC 60870-5-104 based SCADA networks. *IEEE Power and Energy Society General Meeting*.

Yang, Y., McLaughlin, K., Sezer, S., Littler, T., Im, E. G., Pranggono, B., & Wang, H. F. (2014). Multiattribute SCADA-specific intrusion detection system for power networks. *IEEE Transactions on Power Delivery*, *29*(3), 1092–1102.