**REFERENCES**

1. J. F. Clemente, “No cyber security for critical energy infrastructure,” Ph.D.dissertation, Naval Postgraduate School, 2018.
2. C. Bellinger, S. Sharma, and N. Japkowicz, “One-class versus binary classification: Which and when?” in 2012 11th International Conference on Machine Learning and Applications, vol. 2, 2012, pp. 102–106.
3. M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, “Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things,” IEEE Internet of Things Journal, vol. 6, no. 4, pp. 6822–6834, 2019.
4. I. A. Khan, D. Pi, Z. U. Khan, Y. Hussain, and A. Nawaz, “HML-IDS: A hybrid-multilevel anomaly prediction approach for intrusion detection in SCADA systems,” IEEE Access, vol. 7, pp. 89 507–89 521, 2019.
5. T. K. Das, S. Adepu, and J. Zhou, “Anomaly detection in industrial control systems using logical analysis of data,” Computers & Security, vol. 96, p. 101935, 2020.
6. J. J. Q. Yu, Y. Hou, and V. O. K. Li, “Online False Data Injection Attack Detection With Wavelet Transform and Deep Neural .
7. S. D. Anton, A. Hafner, S. Sinha, and H. Schotten, “Anomaly-based intrusion detection in industrial Data with SVM and random forests,” in the 27thInternational Conference on Software, Telecommunications and ComputerNetworks (SoftCOM). IEEE, 2019.19
8. M. Kravchik and A. Shabtai, “Efficient cyber attack detection in industrial control systems using lightweight neural networks and pca,”IEEE transactions on dependable and secure computing, pp. 1–1, 2021.
9. M. Macas and W. Chunming, “Enhanced cyber-physical security through deep learning techniques,” CEUR Workshop Proceedings, vol.2457, no. 38, 2019.
10. C.-t. Chu, S. Kim, Y.-a. Lin, Y. Yu, G. Bradski, K. Olukotun, and A. Ng,“Map-reduce for machine learning on multicore,” in Advances in Neural Information Processing Systems, B. Scholkopf, J. Platt, and T. Hoffman, ̈Eds., vol. 19. MIT Press, 2007, pp. 281–288.
11. M. M. N. Aboelwafa, K. G. Seddik, M. H. Eldefrawy, Y. Gadallah, and M. Gidlund,“A machine-learning-based technique for false data injection attacks detection in industrial iot,” IEEE Internet of Things Journal, vol. 7, no. 9, pp. 8462–8471, 2020.
12. W. Yan, L. K. Mestha, and M. Abbaszadeh, “Attack detection for securing cyber physical systems,” IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8471–8481,2019.