[16] M. Shokry, A. I. Awad, M. K. Abd-Ellah, and A. A. M. Khalaf, "Systematic survey of advanced metering infrastructure security: Vulnerabilities, attacks, countermeasures, and future vision," *Future Generation Computer Systems*, vol. 136, pp. 358–377, Nov. 2022, doi: 10.1016/j.future.2022.06.013.

[17] A. Goudarzi, F. Ghayoor, M. Waseem, S. Fahad, and I. Traore, "A Survey on IoT-Enabled Smart Grids: Emerging, Applications, Challenges, and Outlook," *Energies (Basel)*, vol. 15, no. 19, p. 6984, Sep. 2022, doi: 10.3390/en15196984.

[18] P. A. Schirmer and I. Mporas, "Non-Intrusive Load Monitoring: A Review," *IEEE Trans Smart Grid*, vol. 14, no. 1, pp. 769–784, Jan. 2023, doi: 10.1109/TSG.2022.3189598.

[19] C. Song, Y. Sun, G. Han, and J. J. P. C. Rodrigues, "Intrusion detection based on hybrid classifiers for smart grid," *Computers & Electrical Engineering*, vol. 93, p. 107212, Jul. 2021, doi: 10.1016/j.compeleceng.2021.107212.

[20] R. Yao, N. Wang, Z. Liu, P. Chen, and X. Sheng, "Intrusion Detection System in the Advanced Metering Infrastructure: A Cross-Layer Feature-Fusion CNN-LSTM-Based Approach," *Sensors*, vol. 21, no. 2, p. 626, Jan. 2021, doi: 10.3390/s21020626.

[21] T. Yang, Y. Liu, and W. Li, "Attack and defence methods in cyber-physical power system," *IET Energy Systems Integration*, vol. 4, no. 2, pp. 159–170, Jun. 2022, doi: 10.1049/esi2.12068.

[22] Z. A. Khan and A. S. Namin, "A Survey of DDOS Attack Detection Techniques for IoT Systems Using BlockChain Technology," *Electronics (Basel)*, vol. 11, no. 23, p. 3892, Nov. 2022, doi: 10.3390/electronics11233892.

[23] Y. Javed, M. Felemban, T. Shawly, J. Kobes, and A. Ghafoor, "A Partition-Driven Integrated Security Architecture for Cyberphysical Systems," *Computer (Long Beach Calif)*, vol. 53, no. 3, pp. 47–56, Mar. 2020, doi: 10.1109/MC.2019.2914906.

[24] L. R. Rabiner, "A tutorial on hidden Markov models and selected applications in speech recognition," *Proceedings of the IEEE*, vol. 77, no. 2, pp. 257–286, 1989, doi: 10.1109/5.18626.

[25] D. Ourston, S. Matzner, W. Stump, and B. Hopkins, "Applications of hidden Markov models to detecting multi-stage network attacks," in *36th Annual Hawaii International Conference on System Sciences, 2003. Proceedings of the*, 2003, p. 10 pp. doi: 10.1109/HICSS.2003.1174909.

[26] S. A. Zonouz, H. Khurana, W. H. Sanders, and T. M. Yardley, "RRE: A Game-Theoretic Intrusion Response and Recovery Engine," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 395–406, Feb. 2014, doi: 10.1109/TPDS.2013.211.

[27] S. Iannucci and S. Abdelwahed, "Model-Based Response Planning Strategies for Autonomic Intrusion Protection," *ACM Transactions on Autonomous and Adaptive Systems*, vol. 13, no. 1, pp. 1–23, Mar. 2018, doi: 10.1145/3168446.

[28] E. Miehling, M. Rasouli, and D. Teneketzis, "A POMDP Approach to the Dynamic Defense of Large-Scale Cyber Networks," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 10, pp. 2490–2505, Oct. 2018, doi: 10.1109/TIFS.2018.2819967.

[29] A. Beynier, F. Charpillet, D. Szer, and A.-I. Mouaddib, "DEC-MDP/POMDP," in *Markov Decision Processes in Artificial Intelligence*, Hoboken, NJ USA: John Wiley & Sons, Inc., 2013, pp. 277–318. doi: 10.1002/9781118557426.ch9.

[30] T. Shawly, A. Elghariani, J. Kobes, and A. Ghafoor, "Architectures for Detecting Interleaved Multi-stage Network Attacks Using Hidden Markov Models," *IEEE Trans Dependable Secure Comput*, pp. 1–1, 2019, doi: 10.1109/TDSC.2019.2948623.

[31] T. Shawly, M. Khayat, A. Elghariani, and A. Ghafoor, "Evaluation of HMM-Based Network Intrusion Detection System for Multiple Multi-Stage Attacks," *IEEE Netw*, vol. 34, no. 3, pp. 240–248, May 2020, doi: 10.1109/MNET.001.1900426.

[32] Snort intrusion detection/prevention system. [Online]. Available: https://www.snort.org