6th International Conference on IoT Based Control Networks and Intelligent Systems (ICICNIS), Bengaluru, India, 15-17 December 2025

Cybersecurity in smart grids using machine learning: A systematic literature review

Nelufule, Nthatheni
Council for Scientific and Industrial Research (CSIR)
Meiring Naude Drive, Pretoria, 0184
Email: NNelufule@csir.co.za

The Smart Grids due to their reliance to the connectedness of Internet of Things technologies, advanced metering infrastructure, and real-time communication are faced with significant cybersecurity and privacy risks. In this work a synthesized insights from recent literatures are presented which critically evaluate Machine Learning, Deep Learning, and privacy-preserving techniques for securing smart grids against cyber-attacks. The critical analysis of this review spans across several themes and topics such as ensemble ML models, federated learning, graph neural networks and blockchain-based protocols, scalability, and privacy-aware communication frameworks. However, there are several limitations such as reliance on simulated datasets, computational complexity, adversarial vulnerabilities, scalability issues, and lack of real-time data validation which limits their practical deployment in a real-world environment. This survey has also proposed some research solutions such as standardized real-world datasets, lightweight algorithms, adversarial training, explainable AI, and interoperable blockchain frameworks to enhance robustness, scalability, and trust. This study addresses key research questions on the effectiveness of learning based techniques, and the role of emerging technologies such as 5G technologies and explainable AI in securing a smart grids environment.