IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429

Volume 5, Issue 1, September 2025

Impact Factor: 7.67

Adversarial Autoencoding Framework for Unsupervised Cyber Intrusion Detection in Smart Grid Distribution with Renewable Energy Integration

Mr. Gajanan B. Kadam[1], Prof. Sushil V. Kulkarni[2], Prof. Vijay M. Chandode[3]

M.B.E.S. Society's College of Engineering, Ambajogai, India[1]

Professor, Department of CS-IT, M.B.E.S. Society's College of Engineering, Ambajogai, India[2]

Head of Department, Department of CS-IT, M.B.E.S. Society's College of Engineering, Ambajogai, India[3]

Abstract: *The increasing integration and advancement of digital technologies in power distribution grids has significantly enhanced operational efficiency, yet it has simultaneously heightened vulnerability to various cyber attacks that pose severe risks. This paper presents an innovative and cutting-edge approach that utilizes Unsupervised Adversarial Autoencoders (UAAEs) specifically for the critical detection of cyber threats that are targeting power distribution systems. By leveraging the powerful capabilities of unsupervised learning, the proposed model effectively identifies and discerns anomalies without the requirement for labeled data, which is frequently scarce and hard to acquire in many real-world scenarios. The UAAE architecture is made up of a generator and a discriminator that work collaboratively to learn and establish the normal operational patterns of the grid, which enables the effective detection of deviations that are indicative of potential cyber attacks. Through extensive and rigorous experimentation on simulated datasets reflecting the operations of power distribution grids, the proposed method demonstrates superior performance in terms of accuracy and recall when compared to traditional detection mechanisms that are currently in use. Additionally, the implementation of adversarial training significantly enhances the model's robustness against evasion tactics that are often employed by sophisticated and determined attackers. The findings underscore the potential of UAAEs as a pivotal and vital tool for enhancing the cybersecurity posture of power distribution grids, ultimately contributing to more resilient and secure energy infrastructures that can better withstand cyber threats. Through this approach, we aim to significantly bolster the defenses against potential vulnerabilities in the increasingly digital landscape of power distribution systems.*

Keywords: Unsupervised Learning, Adversarial Autoencoder, Cyber Attack Detection, Power Distribution Grids, Anomaly Detection, Cybersecurity, Robustness, Energy Infrastructure, Machine Learning

DOI: 10.48175/IJARSCT-28908